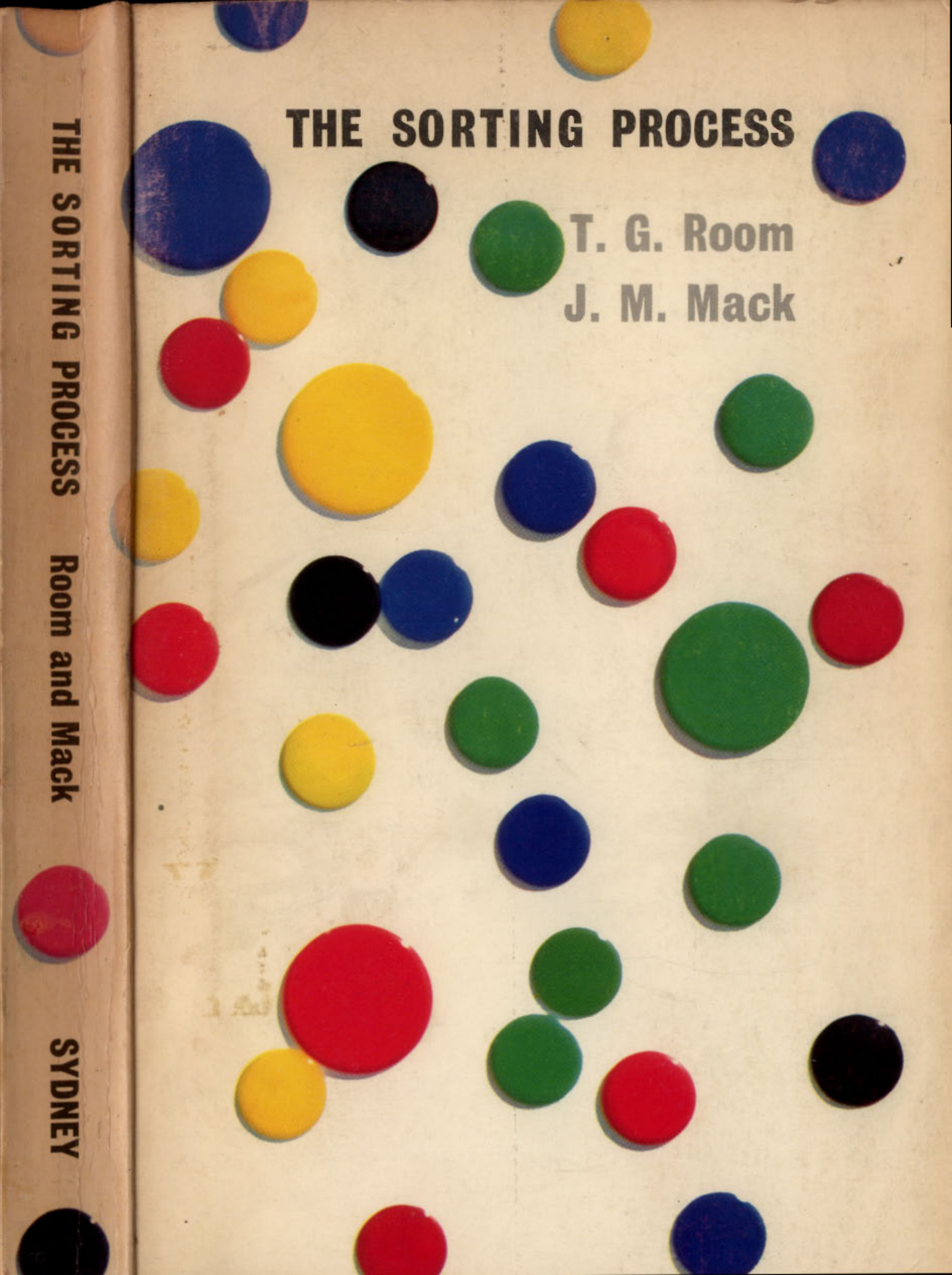


THE SORTING PROCESS

T. G. Room
J. M. Mack

THE SORTING PROCESS Room and Mack SYDNEY

The Sorting Process

a study in mathematical structure

by

T. G. ROOM
Professor of Pure Mathematics
University of Sydney

J. M. MACK
Lecturer in Mathematics
University of Sydney

1966
SYDNEY UNIVERSITY PRESS
London : Methuen

Sydney University Press

PRESS BUILDING UNIVERSITY OF SYDNEY N.S.W. AUSTRALIA

U.S.A.: PENNSYLVANIA STATE UNIVERSITY PRESS

WELLINGTON: PRICE MILBURN AND COMPANY LIMITED

ELSEWHERE: METHUEN AND COMPANY LIMITED, LONDON

AND THEIR AGENTS

© T. G. Room, J. M. Mack, 1966

This book is supported by funds from
the Eleanor Sophia Wood Bequest

Registered in Australia for transmission by post as a book
PRINTED IN AUSTRALIA BY HALSTEAD PRESS, SYDNEY

PREFACE

This book has grown out of lectures given by the authors to groups of secondary school teachers in N.S.W. after the introduction of a new mathematics syllabus which included for the first time some exploration of the simplest properties of sets. The authors found no lack of interest in the neat little system of relations among subsets derivable from observations of a sorting process, but when the last exercise in Boolean algebra had been completed, it was apparent to them that the class felt that the subject was finished: there was nothing to add. The authors take the opposite view: elementary set theory opens up a small but fascinating region of mathematics whose development is well within the competence of the better high school student.

In their discussion with the teachers the authors were impressed by the great difficulty that the teachers experienced in realising the origin and significance of these new mathematical ideas. For this reason, the first four chapters are developed slowly. Each step is introduced by a discussion of an observable property of an easily visualised collection of objects, and the path from the observations to the mathematical concept is carefully traced. The object of the next four chapters is to exhibit the identity of structure between the algebra of finite sets and some quite differently based mathematical systems, any of which may be used as a 'model' for the others. These identities of structure are intended to lead to a better understanding on the one hand of the organisation of the subsets of a set, and on the other of the properties of the other mathematical systems. In addition, the algebra involved is a source of exercises calling for the display of ingenuity in manipulative work when not all the ordinary rules of arithmetic apply. While some of the ideas may at first seem complicated and elusive, the manipulative work rarely involves any but the simplest of algebraic operations.

The final two chapters are meant to emphasise the care that has to be exercised in attempting to apply the ideas derived from physically observable (finite) sets to sets which can have no physical counterpart, but can be described and defined only mathematically.

In order to illustrate the way in which mathematical ideas grow, one example is developed at some length (Chapter 8, part II). An algebraic system is devised which represents the physical circumstances in which, instead of the usual two states ('in' and 'out'), we recognise three states 'we know it is in', 'we know it is out', 'we do not know whether it is in or out'. Very much in the same way as the study of quadratic equations leads from problems of finding the numbers of things which satisfy some assigned physical conditions to the invention of the physically non-significant complex numbers, this broadening of the physical basis for set-algebra leads to a system in which every pair of subsets has a non-empty intersection, which is either a 'tangible' or a 'fictitious' subset.

In brief, this book is meant to show by illustration from the small and easily comprehended field of finite set relations the way in which mathematics develops from its origins in the co-ordination of physically observed relations, through the representation of these relations by various mathematical models, up to the evolution of branches of pure mathematics which bear little trace of their practical beginnings.

T.G.R., J.M.M.

CONTENTS

Page

List of Symbols

Chapter 1 THE SORTING PROCESS

1.1 Introduction 1
1.2 Some examples of sorting processes 1
1.3 One particular collection 3
1.4 Introducing standard words and phrases; symbols 5
1.5 A relation between subsets 8
1.6 Introduction of diagrams 10
1.7 Methods of demonstrating a proof 14
1.8 Care in the use of diagrams 15
1.9 Summary 17

Chapter 2 SETS AND SET-OPERATIONS

2.1 The intersection of two subsets 19
2.2 Intersections of three subsets 22
2.3 The union of two subsets 26
2.4 Union of three subsets 27
2.5 The complement of a subset 29
2.6 Subset formation involving the operations of union, intersection and complementation 29
2.7 Two further operations on subsets 37
2.8 Primary subsets of a set 41
2.9 Duality 43
2.10 Summary. Formulation of a mathematical system 44

Chapter 3 DESCRIPTIONS AND STATEMENTS

3.1 Introduction 47
3.2 The negation of a statement 47
3.3 Conjunction and disjunction of statements 49
3.4 Interpretation of the relation $\subseteq$ 51
3.5 Necessity conditions 52
3.6 Necessary and sufficient conditions 54
3.7 Direct and indirect methods of proof 56
3.8 The logician's term 'implies' 58
3.9 Summary 61

Chapter 4 BOOLEAN ALGEBRA

4.1 A change of viewpoint 64
4.2 Specifying relations and operations 66
4.3 Construction and use of a mathematical model 69
4.4 An axiom system for Boolean algebra 71
4.5 Introduction of the partial ordering ⊆ 73
4.6 Reducing the number of axioms 75
4.7 Summary 76

Chapter 5 H.C.F. AND L.C.M.

5.1 Introduction 78
5.2 Factorisation as a sorting process 78
5.3 The H.C.F. operation 79
5.4 The L.C.M. operation 82
5.5 Distributive relations 83
5.6 Complementation 85

Chapter 6 SETS AND BINARY ARITHMETIC

6.1 Twenty questions 88
6.2 Labelling by binary numbers 90
6.3 Binary numbers and the characteristic sequences 96
6.4 The index number of a subset 98

Chapter 7 SETS AND BINARY ALGEBRA

7.1 The analogy with Cartesian Geometry 101
7.2 Binary algebra 103
7.3 Binary algebra and set operations 105
7.4 Binary algebra and set relations 111
7.5 Characteristic functions 114
7.6 Another algebraic model: rational characteristic functions 116
7.7 The synthesis and analysis of characteristic functions 118
7.8 Boolean algebra 120

Appendix

7.9 An application of matrix algebra 122

Chapter 8 ALLOWING FOR UNCERTAINTY AND IGNORANCE

8.1 The process of 'generalisation' 127

I *Allowing for uncertainty*

8.2 Numerical data for sets 129
8.3 Probabilities 131
8.4 Independent probabilities 132
8.5 A proposed model which proves to be inconsistent 135
8.6 Characteristic functions and probabilities 136

II *Allowing for ignorance*

8.7 An analysis of the physical problem 140
8.8 Relations among subsets 145
8.9 Ternary algebra 147
8.10 Intersections and unions; tangible and fictitious subsets 152
8.11 Ordinary set relations and ternary algebra 157

Chapter 9 NON-FINITE SETS—DENUMERABLE SETS
9.1 The description 'non-finite' 163
9.2 The idea of one-to-one correspondence 164
9.3 The counting or natural numbers 166
9.4 The non-finite set **N** of counting numbers 167
9.5 Various methods for obtaining subsets of **N** 168
9.6 The relations $\subset$ and $\simeq$ between subsets of **N** 172
9.7 Denumerable sets 174
9.8 The set **P*** of r-plets ($r = 2, 3, \ldots$) of counting numbers 176

Chapter 10 NON-FINITE SETS—NON-DENUMERABLE SETS
10.1 The set $\mathscr{Q}$ of quadratic surds 179
10.2 Polynomials of orders three and greater: algebraic numbers 181
10.3 The sets A and **A** 184
10.4 The set **R** of real numbers: the continuum 189

APPENDIX
Solutions to and comments on some of the exercises 193

INDEX 233

LIST OF SYMBOLS

SET NOTATION	*Page*
$\{\ldots.\}$	6
$\mathbf{U}$	6
$a, b, c, \ldots$	7
A, B, C, . . .	7
k:	7
$\emptyset$	21
$\mathbf{[}n\mathbf{]}$	92, 94
$A^{\surd}, A^{0}, A^{\times}, \ldots$	142
$<\ldots>$	174

SET RELATIONS	
$\in$	7
$\notin$	9
$\bumpeq$	8
$\not\bumpeq$	9
$\subset, \not\subset$	9
$\subseteq, \not\subseteq$	9
$\supset$	9
$\simeq$	165
$\prec$	173

SET OPERATIONS	
$\cap$	19
$\cup$	26
$\sim$	29
$-$	38
σ	39
$+$	74

STATEMENT ALGEBRA	*Page*
$p, q, r, \ldots$	47
$\sim p$	48
$\bumpeq$	48
$\wedge$	49
$\vee$	50
$\Rightarrow$	52, 53
$\Leftrightarrow$	55
$\rightarrow$	59
$\leftrightarrow$	61

BOOLEAN ALGEBRA	
$\leftrightharpoons$	66

ALGEBRAIC REPRESENTATIONS	
$=$	103
$\equiv$	103
$\boldsymbol{=}$	103
$c(x)$	105
$\bar{x}$	105
$m(x, y)$	106
$u(x, y)$	106
$d(x, y)$	109
$s(x, y)$	109
$j(x, y)$	109
$n(x, y)$	110
$\downarrow$	121

NON-FINITE SETS	
$\mathbf{N}$	167
$\mathbf{I}$	168
$\mathbf{Q}$	168
$\mathbf{R}$	168
$\mathbf{P}$	174
$\mathbf{P}^*$	176
$\mathcal{Q}$	179
$\mathbf{A}$	184
A	184
$h(p)$	186

Chapter 1

THE SORTING PROCESS

1.1 *Introduction*

This book is a study of the properties of a very simple mathematical system. We shall construct this system by studying a reasonably common process—that of classifying or sorting in some way the objects in a collection. All the sorting processes thus considered may be described as follows. Certain properties are observed to be possessed by some of the objects, and it is desired to find all the objects possessing these properties. Clearly a given collection may be sorted in many ways, each determined by the particular property (or properties) of interest at that time.

Initially, we shall always regard our objects as constituting a collection, or heap, or pile, or any other collective noun whose meaning carries no connotation either of number or of a sense of arrangement. We do this to emphasise that we shall not be concerned (at least in the first few chapters) with counting or arranging. Each of these processes is properly applicable to a given collection, but neither is determined by the individual characteristics of the objects forming that collection, and it is precisely with these characteristics that we are concerned. Thus, although in any particular example we could count the number of objects involved, and although we may be obliged to list the objects in order to indicate their respective properties, these are both irrelevant as far as our interest in the objects themselves is concerned.

On the other hand, notice immediately that we should find any collection of identical objects extremely uninteresting, for we could never produce an applicable sorting criterion. The rarity of identical objects of any kind assures us of an interest in almost every collection of real objects.

1.2 *Some examples of sorting processes*

Given a particular heap, an instruction to sort the heap carries with it, as we said before, an understanding of the classifications to be employed in the process. For example, a mail sorter at a post office sorts the letters posted there according to the destination of each letter. Clearly, here, no other sorting criterion is involved (provided all letters are properly addressed and carry the correct amount of postage). However, we may readily offer an example in which a given collection may have many different sorting processes applied to it, depending on the intention of the sorter.

Suppose a stamp-collector acquires a large packet of stamps. If he has a good memory, and knows what stamps he already possesses, then his first step may be to sort out the stamps which are not identical with those already in his possession. Otherwise, his first step may be a sorting of the packet into various heaps, each heap containing stamps having a common country of origin. Some collectors care little for a country classification, and prefer to sort according to design motif—hence, say, all stamps depicting birds will make one heap, all stamps depicting aeroplanes or perhaps commemorating famous flights would form another, and so on, irrespective of country of origin. Still other collectors require unused stamps, and so would initially sort to discard all used stamps. Several other possibilities exist for an initial sorting.

The sorting process here will not necessarily stop after one step. For example, sorting according to country of origin may be followed by sorting according to year or period of issue, and then by a classification into unused or used varieties.

Having in mind our intentions motivating a sorting process, we realise that it may not be necessary to observe minutely each object in a heap. Indeed, we may not wish to record a very obvious property of an object if we are temporarily uninterested in that particular aspect of the objects. For example, returning to the philatelist and his packet of stamps, his first step, before any sorting (and motivated possibly by a desire to avoid unnecessarily handling his stamps) may well be to place each stamp individually in a small envelope (or packet), and then to record on the outside of the container the relevant properties of its content.

Recalling the sorting processes previously mentioned, a typical record would be: 'The enclosed stamp comes from Ecuador. It is unused, it has a picture of a bird on it and was issued in 1948'. Of course, one would seldom bother to write at such length, and in all probability one would read simply 'Ecuador, unused, bird, 1948'. (Certainly such an abbreviated note is mere nonsense to others unless its meaning is explained—we shall have reason later to elaborate this remark.) For the stamp-collector's initial purposes, the heap of labelled containers is completely satisfactory.

In general, we have the following situation: given a heap of objects and various sorting criteria, it will be entirely satisfactory to replace the real objects by a set of labels, each label corresponding precisely to one object, and having on it a list of the relevant properties possessed by that object. If additional properties are required at any stage, we simply examine the real object and add the result of our observation to the list of properties on its label. In other words, we have noticed that it is not always necessary to have a heap of objects present in order to discuss their properties and so sort the heap. Labels or descriptions, each carrying relevant information on one object, can adequately enable us to answer questions concerning the original collection.

1.3 *One particular collection*

We shall take one easily visualised heap of objects, for which we specify and carefully list various attributes of each of the objects, so that we may refer to it whenever we need the support of a physical image of a collection in analysing the properties or devising or applying techniques. At a certain school, we choose a particular class of girls and boys, and we shall study some of the characteristic properties of the pupils. By going to the school, and observing the class, we can compile a great deal of information. To begin, it is unlikely that any two of the children will have even similar features, and so we should have no difficulty in identifying each child. We could do as well by photographing each child, if we were interested solely in sorting according to, say, facial shape. If our interest extends to noting simple things such as whether or not a child wears glasses, or is right-handed, a moment's observation would suffice. But if we had decided in advance which properties we proposed to investigate, there would have been no need for us to travel out to observe the class. We would be quite satisfied had we written to the class teacher and said 'Please send us a photograph of each child in the class. On the back of each photograph, state whether the child appearing in it possesses the following properties'—and then would follow a list of the relevant properties. Equally well, we could have asked for a list of names, instead of photographs. Then, of course, we should not have been able to associate a child with the child's name, so that all our deductions could only be applied to the children after we had made that association. Nevertheless, a name-list will clearly be adequate for our sorting processes. We are not concerned with the way in which the name-list appears. In fact, our list came as follows—in the form of a 'plan' of the classroom.

Jack	*Isobel*	*Evelyn*	*Vera*
Quentin	*Charles*	*Yolande*	*Percy*
Anne	*Lucy*	*Olive*	*Dorothy*
Nancy	*Una*	*Karen*	*Tom*
Fred	*Bill*	*Susan*	*Harry*
Richard	*Warren*	*Geoff*	*Mary*

We are not at present interested in the numbers of children, girls, or boys (and so we shan't bother to find out). The information we are seeking came in fact in the following 'sign language' form: beside each child's name there appeared a list of symbols whose meaning was self-evident. Each girl was characterised by ' 🚺 ', each boy by ' 🚹 '. Spectacle-wearers carried the mark ' 👓 ', left-handed writers were identified by '\' and right-handed ones by '/' (indicating the usual slope of pen or pencil in each case). We are able to produce labels, one for each child (say an ordinary tag), on which we write down the information given. Here we shall simply make a list of names, and put down beside each name the signs we have been given for that child.

Anne	🚺 \
Bill	🚹 \
Charles	🚹 👓 /
Dorothy	🚺 /
Evelyn	🚺 /
Fred	🚹 👓 \
Geoff	🚹 /
Harry	🚹 👓 /
Isobel	🚺 /
Jack	🚹 \
Karen	🚺 /
Lucy	🚺 \
Mary	🚺 \
Nancy	🚺 /
Olive	🚺 /
Percy	🚹 /
Quentin	🚹 👓 /
Richard	🚹 /
Susan	🚺 /
Tom	🚹 /
Una	🚺 /
Vera	🚺 \
Warren	🚹 /
Yolande	🚺 /

For example, we know that Harry is a boy who wears spectacles and is right-handed. [Notice that the signs appearing after each name could have been printed in any order; we have nothing to gain at present by arranging them in a particular way.]

What, now, does a sorting process involve? Precisely a change of viewpoint, as follows: instead of associating with each child its list of properties, we associate with a specific property the collection of children possessing it. Thus, sorting the class into girls or boys means making two new lists, one of names carrying the sign 🚺 and the other of those marked 🚹. So we have:

List of Girls

Yolande *Vera* *Una* *Susan* *Olive*
Nancy *Mary* *Lucy* *Karen* *Isobel*
Evelyn *Dorothy* *Anne*

Similarly, we may sort and obtain:

List of Spectacle-wearers

Charles *Fred* *Harry* *Quentin*

Thus a sorting process is simply a way of distinguishing some of the children in the class, depending on their possessing a certain property or satisfying a particular description. Each sorting gives us a list containing some of the names in the original list.

1.4 *Introducing standard words and phrases; symbols*

We shall find the writing out of lists quite tiresome, and so, instead of doing this, we propose to explain a simpler method of referring to them. Simplicity alone might justify our new method, but experience teaches us that it is also very convenient to develop a certain basic vocabulary—to 'standardise' the words and phrases we use, and to adopt a specific notation to denote (where useful) these words and phrases.

Firstly then, we introduce some common words whose meaning, when used in the sequel, will be always in the sense explained now. The word SET will be used to denote the original heap, pile or collection of objects. In future we shall always refer to a set of objects.

A SUBSET is a part of a set; therefore it will be used to refer to any portion of a heap, pile, collection, etc.

ELEMENT or MEMBER will in future replace 'object'—we shall refer to 'the elements of a set' rather than to 'the objects in a collection'.

Finally, in order to describe the relation between 'object' and 'heap', or 'element' and 'set', we shall use any of the phrases 'is a member of', 'is an element of', 'belongs to'.

Thus, no matter what the real nature of the original collection, it will always be called a set, it will have subsets, and it will consist of elements or members. For example, we may say of our class:

The basic set is the set of children in the class.

Anne is a member of the set of children in the class.

The girls in our basic set form a subset of that set.

Anne is a member of the subset of girls.

To avoid writing at length, we introduce a standard notation the systematic use of which will enable us to express ourselves precisely and concisely.

Initially, the set of children in the class was given as a 'class plan'; then as a list of names. Henceforth, we shall specify a set by enclosing the names of its elements within braces—thus the set of children in the class is the set {. . . .}, where, within the braces, we write, in any order, in any way at all, the names of the children in the class, each name written once only. For example, the subset of children who wear spectacles is {*Quentin*, *Charles*, *Harry*, *Fred*}.

When we wish to refer to a particular set without wishing to specify again its elements, we shall label it with a single block capital—thus the basic set (whatever it may be) will be given the label U (because it is usually referred to as the universal set or universe under consideration), and we would then speak of U, the set of children in the class. Subsets of U will be given their identifying labels as we have need of them.

Writing out names of elements in full is also rather tiresome, so we look for a way of abbreviating such names. Using the class of children as an example, we notice that no two names begin with the same letter of the alphabet. Therefore, specifying an initial letter specifies the corresponding name and so specifies a particular child. Hence we may save much writing simply by denoting a child by the initial letter of its Christian name. The set U will then be $\{A, B, C, \ldots, W, Y\}$, or $\{B, Y, W, D, \ldots\}$, where the braces contain in any order the twenty-four initial letters of the children's names. These letters are printed in a line because it is convenient to do so, and because in written or verbal communication, words appear sequentially, not simultaneously. When we want to emphasise that a set consists of its members, and that no preference is attached to any particular member by mentioning it before another, we must point out that the order in which the members are mentioned is not significant.

Our use of initial letters as representative symbols for the elements of a set had a clear motivation. The requirements such symbols must satisfy are that they are easy to use, and serve as distinguishing marks for the real objects, so that each symbol is identified with precisely one object. In the notation in common use, small letters *a*, *b*, *c*, . . . always denote elements, and capitals A, B, . . . , U denote sets or subsets.

We have so far adopted the convention that a set will be denoted by {. . . .} where between the braces there is a list of members of the set. The essential part of the notation is the braces, and if the set can be defined by a statement of a characteristic property, we could equally well denote the set by braces enclosing this statement. If in our example we wish to refer to the set of girls in U, without listing its elements, we may agree to write it also as {all elements of U who are girls}, or in some similar descriptive form. We eliminate possible confusion by specifying a standard form for such descriptive representations. An arbitrary element of a set (or subset) will be denoted by *k*. We write

{all elements *k* such that *k* is a child in the class who is a girl}

or

{all elements *k* such that *k* is an element of U who is a girl}

and finally in the form

{*k* : *k* belongs to U and *k* is a girl},

where '*k*:' is read 'all elements *k* such that'.

The phrase 'belongs to' occurs so frequently that we denote it by the symbol $\in$—thus $k \in \mathrm{U}$ is read '*k* belongs to U' or '*k* is an element of U'.

So we have the set of girls in the class expressible in the form $\{k : k \in \mathrm{U}$ and k is a girl$\}$.

The general descriptive form of writing a set is {*k* : *k* has certain properties}, and for a subset of U is $\{k : k \in \mathrm{U}$ and k has certain properties$\}$.

We now have various ways of referring to a given set. Thus the set of spectacle-wearers in the class is the same set as the set {*Fred*, *Charles*, *Harry*, *Quentin*}, which is the same set as $\{F, C, H, Q\}$ which is the same set as $\{k : k \in \mathrm{U}$ and k is a spectacle-wearer$\}$. Let S be the symbol denoting this subset. If we define '$\simeq$' to mean 'is the same set as', we may write

S $\simeq$ the subset of spectacle-wearers in the class,
$\simeq$ {*Quentin*, *Charles*, *Harry*, *Fred*},
$\simeq \{H, F, C, Q\}$,
$\simeq \{k : k \in \mathrm{U}$ and k is a spectacle-wearer$\}$.

Exercise 1. Using the set U of children given in the text, find the various ways of writing the following subsets of U:

(a) L, the subset of children who are left-handed,
(b) the subset {*Fred*, *Jack*, *Bill*},
(c) the subset $\{B, F, J, L, M, N\}$.

Exercise 2. According to our definition, to specify a set as $\{a, a, a\}$ is nonsense. Why? Does {dog, dog, cat} specify a set? If not, in what ways could you denote a set consisting of two dogs and a cat?

In the sequel, elements of a set U will be denoted by $a, b, c, \ldots$ etc.; subsets of U by A, B, C, . . . etc. An unspecified element of a set will be denoted by k. In the special case where U is the set of children in the class, we label the following subsets:

G $\simeq$ the set of girls,
B $\simeq$ the set of boys,
S $\simeq$ the set of spectacle-wearers,
L $\simeq$ the set of left-handed writers,
R $\simeq$ the set of right-handed writers,
C $\simeq$ the set of children whose name commences with a consonant,
V $\simeq$ the set of children whose name commences with a vowel,
P $\simeq$ the set of children whose name (as given) is four letters long.

1.5 *A relation between subsets*

The statement 'k is a member of U', or equivalently, '$k \in \mathrm{U}$', is an expression of a mathematical relationship. The symbol '$\in$' represents a relation connecting the two entities denoted by the symbols k (an element-symbol) and U (a set-symbol). Another relationship, but this time one connecting two sets, already suggests itself. It is the connection between a subset A of a set U and the set U. Every element $k \in \mathrm{A}$ is clearly an element of U, and we use the phrase 'is contained in', with symbol '$\subset$' to denote this relation. Thus for our set U of children, we have all the relations $G \subset U$, $B \subset U, \dots, V \subset U$, where G, B, . . . , V are as specified before. We read $G \subset U$ as either 'G is a subset of U' or 'G is contained in U'.

Notice, however, that in our example every element of V is an element of G, for

$$V \bumpeq \{\textit{Anne}, \textit{Evelyn}, \textit{Isobel}, \textit{Olive}, \textit{Una}\}.$$

Thus V is a subset of G, and we again write $V \subset G$. In general if, for any set U and two of its subsets, A, B say, we may state 'every element of A is an element of B', then we may also write this as $A \subset B$.

Usually, if $A \subset B$, then there will be elements of B which are not elements of A. For example, *Dorothy* is an element of G, but not of V. When that is so, we say A is a **proper subset** of B. Sometimes it happens that A and B, although defined in seemingly different ways (say as the elements satisfying distinct descriptions) actually have the same elements; i.e. A is the same set as B. We then write (using a notation introduced earlier) $A \bumpeq B$. If we wish to specify that A is a proper subset of B, we write $A \subset B$, while if we are willing to admit also the possibility of A and B being one and the same set, we shall write $A \subseteq B$.

We complete this section with a list of the symbols we have introduced, together with a few new ones:

A, B, C, . . . , U		Symbols for sets or subsets
a, *b*, *c*, . . . , *k*		Members or elements of sets
$\in$	$k \in A$	*k* is an element of A, or *k* belongs to A
$\bumpeq$	$A \bumpeq B$	A is the same set as B
$\subset$	$A \subset B$	A is a proper subset of B
$\supset$	$B \supset A$	B contains A as a proper subset
$\subseteq$	$A \subseteq B$	A is a subset of B and may be the same as B
$\notin$	$k \notin A$	*k* is not an element of A
$\not\bumpeq$	$A \not\bumpeq B$	A is not the same set as B
$\nsubseteq$	$A \nsubseteq B$	A is not a subset of B, i.e., there is at least one element of A that is not an element of B
$\not\subset$	$A \not\subset B$	A is not a proper subset of B.

Exercise 3. If of two subsets A, B of a set U, we have $A \not\subset B$, does it necessarily follow either that $A \bumpeq B$ or that $B \subset A$?

Exercise 4. Referring to the set U of children of the text, write down the correct relation between the following pairs: G and U, V and G, S and B, L and C, *Bill* and C, *Geoff* and V, R and B, {*Tom*, *Una*} and R, {*Jack*, *Lucy*, *Vera*} and L, {*Quentin*, *Fred*} and L.

Exercise 5. Let U $\doteqdot$ the set of letters of the alphabet. V, C here will denote respectively the subsets of vowels and consonants. Further

A $\doteqdot$ set of all letters whose capital form is composed of straight strokes
W $\doteqdot$ set of letters in 'walnut'
S $\doteqdot$ set of letters in 'syzygy'
Z $\doteqdot$ $\{z\}$
N $\doteqdot$ set of all letters whose names do not begin with themselves.

Find the relations between all pairs chosen from V, C, A, W, S, N, and Z. Which subsets contain H $\doteqdot$ $\{h\}$?

The relation $\subseteq$ between subsets can be interpreted as an element-property as follows: A $\subseteq$ B means 'if we know k is an element of A, then we know also that k is an element of B'. Similarly, A $\doteqdot$ B means 'the elements of A are precisely those of B'. Later we shall study closely these relations.

1.6 *Introduction of diagrams*

The words, symbols, and notation discussed so far have been introduced for two reasons. Firstly, by consistent use of them we shall simplify the written form of various statements and descriptions. Secondly, we have a method of description that is applicable to arbitrary collections of objects. For example, the statement 'A $\subseteq$ U' is a statement about any subset of a given universal set U, but there is no reference to, or description of, either U or A, as we have for instance in the statement 'The girls form part of the class of children'.

Clearly, we need both of the above properties, i.e. simplicity and generality, if we wish to discuss properties of a set and its subsets, that is, if we wish to explain in words the conclusions we obtain by thinking about these properties. When symbols, and not words, are used in explanation, they should be used for economy of expression and clarification of what we wish to say. A sensible choice and use of symbols not only does this, but sometimes suggests that other results, not yet established, may be true. So it is, for example, with the correct use of words in an explanation. A person who cannot use a spoken or written language competently will find it difficult to explain his thoughts to others.

Quite often in everyday life, a picture, or sketch, will convey relevant or necessary information just as efficiently, and even more directly, than a verbal or written explanation. (One has only to examine the format of advertisements in a newspaper to verify this.) Indeed, it is often convenient to think or imagine in pictorial, or geometrical, language instead of in words. Therefore we are naturally led to inquire if there is a pictorial or diagrammatic language (symbolism) appropriate to our subject—can we represent lists by diagrams in such a way that relations between lists are represented by, or reflected in, corresponding properties of our diagrams? The answer is 'yes', and the motivation leading to the diagrams is a very simple one—lists shall correspond to regions in such a way that inclusion of one list in another shall correspond to inclusion of one region in another. We now develop and explain this idea.

Using our basic set U, we list the elements of G:

Anne
Dorothy
Evelyn
Isobel
Karen
Lucy
Mary
Nancy
Olive
Susan
Una
Vera
Yolande

and now the elements of V:

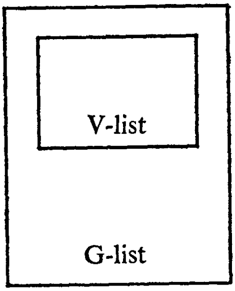
Anne
Evelyn
Isobel
Olive
Una

We can do this more economically by writing the list for G in any way in which the elements of V appear together, so that we can indicate the V-list on the G-list. For example, if we have G:

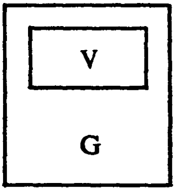
$$\left.\begin{array}{l}\textit{Anne}\\ \textit{Evelyn}\\ \textit{Isobel}\\ \textit{Olive}\\ \textit{Una}\end{array}\right\}\ \text{V-list}$$

Dorothy
Karen
Lucy
Mary
Nancy
Susan
Vera
Yolande

we may indicate the elements of V as above. But we prefer to use the following method. Enclose the G-list in a rectangle, and the V-list within a rectangle, as follows:

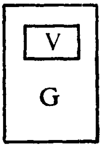


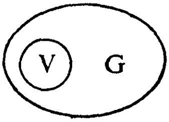
where we suppose the lists written out in full. If we regard the inner rectangle as representing V (and so label it V) and the whole outer rectangle as representing G (and so label it G) then we may omit the lists, and use the diagram:

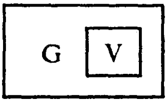


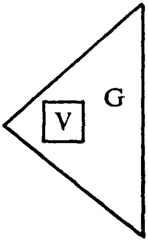
to give physical meaning to the relation $V \subset G$.

We used rectangles because they fitted the shape of our lists. If we had written our lists in some other shape, our figures would have had another shape. Clearly, shape and size are immaterial as long as the configuration of shapes corresponding to lists reflects the relations among the lists. Thus $V \subset G$ is expressible as any of the following:



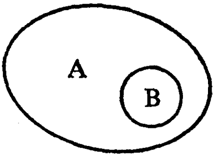




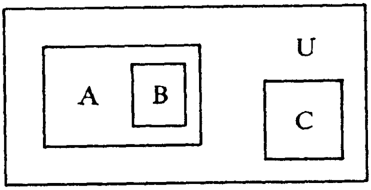


We shall use rectangles systematically, mainly for ease of drawing when several sets are involved.

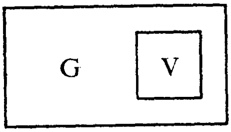
For any set U, the relation $B \subset A$ between two of its subsets may always be represented by a diagram such as the one below:



For any given set U, full information could be recovered by writing in the appropriate regions the lists of names of the elements concerned. Naturally, when we are concerned with U itself, we represent it as a 'frame' in which all other regions, corresponding to its subsets, appear:



When U does not explicitly concern us, i.e. when we deal with certain subsets, we shall usually leave out the region corresponding to it, as we have already done in the diagram:



Diagrams, when used in this way, are often called 'Venn diagrams'.

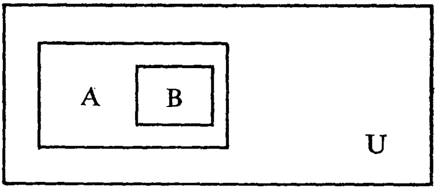
1.7 *Methods of demonstrating a proof*

A 'proof' is a communication by one person to another of the process of thought by which he has convinced himself that whenever a system is described as having certain properties, it has as well some property not included explicitly among these properties. There are several ways in which this communication may be made, as for example, by spoken or written word, by the use of a mutually understood symbolism, or by pictures or diagrams. What is asked of any such communication is that it gives an adequate description of the argument involved, unencumbered by redundant or irrelevant material. If then a proof can be explained simply by using a diagram, we may do so, and we shall do so whenever this method of communication seems to us most satisfactory.

Earlier, however, we remarked that an appropriately chosen symbolism may sometimes suggest results. We must emphasise that all such possible results can only be ignored, or treated as plausible conjectures, until we have either obtained proofs or shown their falsity. Just as people who read carelessly gain wrong impressions or draw incorrect conclusions, so carelessness with symbols leads to invalid results. Unfortunately, there is often a strong temptation to manipulate symbols, or interpret diagrams, while forgetting their roles as representations of some other system, and when that is allowed to happen, we can hardly expect the results of our absent-mindedness to have any application, or even any meaning, when applied to our original system!

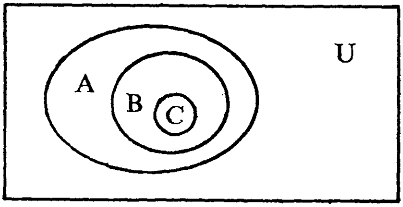
1.8 *Care in the use of diagrams*

We take two simple examples as illustrations of our argument. Suppose we are given that A and B are subsets of U, and no other information about them, but draw the diagram in the following way:



On the basis of our observation of this diagram, we would conclude 'if we are told $A \subset U$ and $B \subset U$ then we know that $B \subset A$'—an obviously false deduction, because, referring back to the physical basis for our statements about sets and inserting the symbols for specific sets in place of the general symbols A and B, we should be saying for example 'If we are told that there is a set of girls in the class and a set of boys in the class, then we know that every girl is a boy'.

Secondly, suppose we have the following diagram:



drawn on the basis of the information $C \subset B$, $B \subset A$. We observe that the region C is part of the region A, and infer the new result, $C \subset A$. If we can answer 'yes' to the following question, 'Does the given information always produce the above configuration?' our diagram is a proof of our inference. A moment's reflection convinces us that 'yes' is indeed the answer. We have in fact found our first theorem in the set-algebra :

If we are told B ⊂ A and C ⊂ B then we know C ⊂ A.

Of course we may offer other versions of the proof. They are all different ways of expressing the same basic observation, that the list of elements of C is part of the list of elements of B, and so (since that is part of the list of elements of A) part of the list of elements of A. For example, from:

Fred	*Fred*	*Fred*
Harry	*Harry*	*Harry*
Charles	*Charles*	*Charles*
Quentin	*Quentin*	*Quentin*
	Bill	*Bill*
	Geoff	*Geoff*
	Jack	*Jack*
	Percy	*Percy*
	Richard	*Richard*
	Tom	*Tom*
	Warren	*Warren*
		Dorothy
		Karen
		Lucy
		Mary
		Nancy
		Susan
		Vera
		Yolande

we deduce S ⊂ B, B ⊂ C, and also S ⊂ C.

The transition from lists to diagrams enables us to concentrate on the relations between lists without the distraction of the lists themselves.

Thus, our first 'new result' is: if, for three subsets A, B, C, of U we have B ⊂ A and C ⊂ B, then C ⊂ A. This expresses a property known as transitivity of the relation 'is contained in'. Common transitive relations are those containing a comparative—for example, if Tom is taller than Bill, and Bill is taller than Fred, we know Tom is taller than Fred, and the relation 'is taller than' is transitive.

Not all relations are transitive. For example, if A $\not\doteq$ B and B $\not\doteq$ C, we certainly cannot always conclude that A $\not\doteq$ C (why?). Alternatively, if Tom is the father of Bill, and Bill is Fred's father, it is certainly false that Tom is Fred's father, hence 'is the father of' is intransitive.

Exercise 6. Discuss whether either of the ordinary geometrical relations 'is parallel to' and 'is perpendicular to' is transitive.

1.9 *Summary*

Our intention has been threefold:

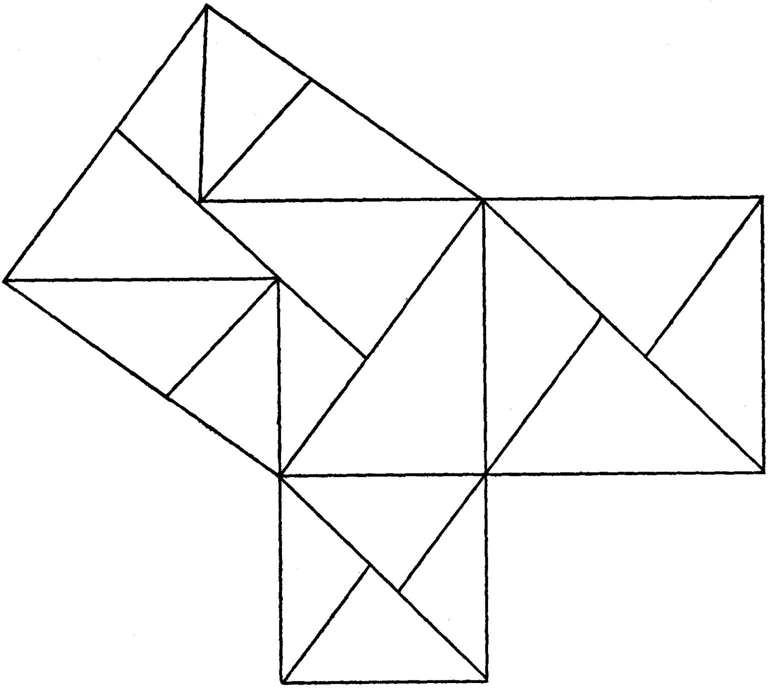
(i) We have slowly developed the notion that one need not deal directly with actual objects in order to discuss some aspects of them. Distinguishable marks, or symbols, invested with relevant information, are sufficient.

(ii) Different types of symbolic representation can usefully be employed, especially if they are capable of representing many varieties of objects. Careful understanding and explanation of any symbolic language are necessary before it can be used in any communication, but we need not necessarily argue in words.

(iii) Systematic use of standard words and phrases can encourage clarity of expression, provided one has taken pains to explain the precise meaning of such standardised words and phrases. Similarly, in any symbolic representation, we choose particular symbols, or particular types of symbols, to convey particular ideas.

(iv) When the significance of the diagrams we have drawn is fully understood, then it is possible to provide a complete proof of some theorems by drawing a diagram which conforms precisely to the description of the relations they represent. That is, the diagram in some cases may be such that the mind can apprehend the sequence of ideas in the proof without at any time having to express the ideas in verbal form.

In this respect, the set diagram appears to differ from the diagram which is drawn as a guide to the verbal formulation of a proof to a theorem in Euclidean geometry. On the other hand, the following diagram could be regarded (against a suitable background of previous theorems) as a complete proof of the Pythagoras theorem.



Chapter 2

SETS AND SET-OPERATIONS

2.1 *The intersection of two subsets*

If we compare the list G of names of girls in the class with the list L of names of left-handed children, we notice that some names are common to both lists, while others appear on one of the two lists, but not on both. We can economise in writing down these lists by writing each of the names common to both lists once only, and by arranging our lists as follows:

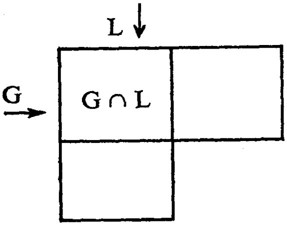
Anne *Lucy* *Mary* *Vera*	*Dorothy* *Evelyn* *Nancy* *Isobel* *Karen* *Olive* *Susan* *Una* *Yolande*
Bill *Fred* *Jack*	

Notice that when depicted as above, our two lists fall naturally into three ‘blocks’. The corner block lists the names of children in the class who are girls and who are left-handed; the right-hand block lists the names of the girls in the class who are not left-handed, while the lower block lists the names of the boys who are left-handed. Now let us look more closely at the corner block. It corresponds to the list obtained by collecting the names that the original lists G, L had in common, and yields a new subset—the set of girls who are left-handed. Naturally, given any two subsets A, B of U, we are therefore led to consider the subset of U consisting of the common members of A and B. We shall name this subset by calling it the **intersection** of the two subsets A and B, and we shall write it as $A \cap B$. Notice immediately that $A \cap B$ is the same set as $B \cap A$, since the common members of A and B are obviously the common members of B and A. In symbols, we have

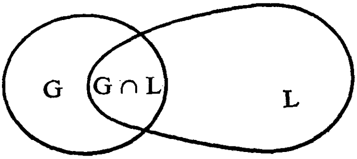
$$A \cap B \bumpeq B \cap A$$

and we say that the operation of forming the intersection of two sets is a **commutative** operation. You will remember that we pointed out earlier that the necessity for making this statement arises only because we have to print one symbol before another and cannot print both simultaneously.

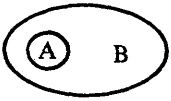
Recalling our original example, we may represent it now by the diagrams:



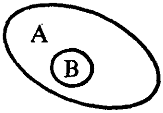
or



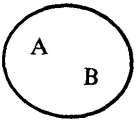
(remembering that the shapes of our regions do not matter). But diagrams of a different appearance may arise when we consider arbitrary subsets A and B of U. In fact, by thinking of all the possible ways two lists can be related to each other, we can draw the following diagrams:



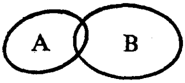
(i) $A \subset B$



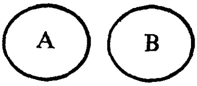
(ii) $B \subset A$



(iii) $B \bumpeq A$



(iv)



(v)

Examples drawn from the class:

(i) $V \subset G$, $V \cap G \bumpeq V$
(ii) $S \subset B$, $B \cap S \bumpeq S$
(iii) $L \bumpeq P$, $L \cap P \bumpeq L \bumpeq P$
(iv) $G \cap L \subset G$, $G \cap L \subset L$
(v) S and G have no common element.

In diagram (i), every element of A belongs to B, and the elements of A are precisely the elements A and B have in common. So here $A \cap B \bumpeq A$. Similarly, in (ii) $A \cap B \bumpeq B$, while in (iii), $A \cap B \bumpeq A \bumpeq B$. (iv) is the case discussed earlier, where $A \cap B$ is a proper subset of A and a proper subset of B. (v) represents the situation where A and B have no common element, so, in order that the symbol $A \cap B$ shall always have a meaning (as we should prefer it to be defined for any two subsets A, B), we introduce the idea of a subset of U which has no elements. This set will be called the **empty set** or the **null set**, and we shall denote it by the symbol $\emptyset$. Regarding subsets of U as lists of elements, the empty set $\emptyset$ corresponds to a blank list. Then, in (v), $A \cap B \bumpeq \emptyset$.

Having introduced $\emptyset$, we must now add two more possibilities to the cases (i)-(v) above, namely

(vi) one, say A, is the empty set $\emptyset$, while $B \not\bumpeq \emptyset$, and
(vii) $A \bumpeq \emptyset$, $B \bumpeq \emptyset$.

If we ask the question 'What elements can any list have in common with a list containing no elements?' the answer is clearly 'none'. Since 'no elements' corresponds to the empty set, we immediately have the answers $A \cap \emptyset \bumpeq \emptyset$, $\emptyset \cap \emptyset \bumpeq \emptyset$, thus covering cases (vi) and (vii).

Hence, for any choice of subsets A, B of U, we have

Definition: The intersection of A and B is the subset $A \cap B$ of U given by

$$\begin{aligned} A \cap B &\bumpeq \{k : k \in A \text{ and } k \in B\} \\ &\bumpeq \{\text{all elements common to A and B}\}, \end{aligned}$$

where

$A \cap B \bumpeq \emptyset$ if A and B have no element in common,
which is always true if one of A, B is $\emptyset$.

If $A \not\bumpeq \emptyset$ and $A \cap B \bumpeq A$, we know that $A \subseteq B$. Since $\emptyset \cap B \bumpeq \emptyset$ for any B it would be a natural generalisation to write $\emptyset \subset B$, and thus to conclude that the empty set has the peculiar characteristic of being a subset of every subset of U. But this is not covered by our original discussion on the symbol $\subset$, which was restricted to subsets containing elements of U. We have a choice: either we start afresh, allowing $\emptyset$ as a subset right from the beginning, or else we incorporate it now by specifying its peculiar property. We choose the latter alternative, and write

for any subset A of U, $\emptyset \subseteq A$.

Now we may write

for any A, if we know $A \cap B \bumpeq A$ then we also know $A \subseteq B$.

Also, we always have the relations $A \cap B \subseteq A$, $A \cap B \subseteq B$.

2.2 *Intersections of three subsets*

We wish now to find the subset consisting of those girls in the class who are left-handed and whose names begin with a consonant. Therefore we write down three lists—the list of girls' names, the list of names of children who are left-handed, and the list of the children's names which begin with a consonant—and identify the names common to all three lists, for these names yield precisely the subset we require. Thus we have:

G	L	C
Lucy	*Lucy*	*Lucy*
Mary	*Mary*	*Mary*
Vera	*Vera*	*Vera*
Anne	*Anne*	*Bill*
Dorothy	*Bill*	*Charles*
Evelyn	*Fred*	*Dorothy*
Isobel	*Jack*	*Fred*
Karen		*Geoff*
Nancy		*Harry*
Olive		*Jack*
Susan		*Karen*
Una		*Nancy*
Yolande		*Percy*
		Quentin
		Richard
		Susan
		Tom
		Warren
		Yolande

and so our required subset is {*Lucy*, *Mary*, *Vera*}.

Starting from three subsets, G, L, C of U, we have formed a new subset, M say, where the members of M are the children in the class who are members of all three subsets G, L and C, i.e.,

$$\begin{aligned} M &\bumpeq \{\text{all children who belong to all three of G, L, C}\} \\ &\bumpeq \{k : k \in G \text{ and } k \in L \text{ and } k \in C\}. \end{aligned}$$

We shall call M the common part or intersection of the three subsets G, L, C.

This suggests that given any three subsets A, B, C of a set U, we can define a new subset, M(A, B, C) say, by the process

$$M(A, B, C) \doteq \{k : k \in A \text{ and } k \in B \text{ and } k \in C\}.$$

We shall call M the intersection of the three subsets A, B, C. Again we point out that M does not depend on the order in which we put A, B, and C, in other words

$$M(A, B, C) \doteq M(A, C, B) \doteq M(\text{any arrangement of } A, B, C).$$

Can we express M in any other way? Let us return to our example, where $M \doteq M(G, L, C)$. Instead of writing down the lists G, L and C, we could have simplified our working, and saved time, by first listing the names common to the subsets G and L, and then comparing this list with that for C. In other words, only the names of girls who are left-handed need be compared with the names beginning with a consonant in order to find the required list. But we already know the children common to G and L; they are precisely the elements of the subset $G \cap L$. The children common to $(G \cap L)$ and C (who will be the elements of M(G, L, C)) form precisely the intersection $(G \cap L) \cap C$. This set, therefore, is the same set as the set M(G, L, C).

So we have

$$M(G, L, C) \doteq (G \cap L) \cap C.$$

But, equally well, we could have found $(L \cap C)$ and then $G \cap (L \cap C)$, which is again the same set as M(G, L, C). Therefore

$$(G \cap L) \cap C \doteq M(G, L, C) \doteq G \cap (L \cap C).$$

In the general case, we shall have

$$M(A, B, C) \doteq (A \cap B) \cap C \doteq A \cap (B \cap C),$$

and remembering that the order in which A, B, C appear is immaterial, we have more equations of the same type, for example

$$M(A, B, C) \doteq M(B, A, C) \doteq (B \cap A) \cap C \doteq B \cap (A \cap C).$$

We draw two conclusions from our argument. Firstly, the common part or intersection M(A, B, C) of three subsets A, B, C can be found by repeated use of the intersection operation $\cap$. Thus

$$M(A, B, C) \doteq (A \cap B) \cap C.$$

Secondly, the order of carrying out the operations $\cap$ on the pairs of subsets is immaterial, as we always produce the set M(A, B, C). But the order of execution of operations is determined symbolically by the insertion of parentheses. For example, $(A \cap B) \cap C$ means first find $A \cap B$, then its intersection with C; while $A \cap (B \cap C)$ means first find $B \cap C$ and then its intersection with A. Since the result is the same, we say that the operation $\cap$ is **associative**, and the symbolic expression of this statement is the sentence:

'If A, B, C are any three subsets of U, then

$$(A \cap B) \cap C \bumpeq A \cap (B \cap C)\text{'.}$$

When an operation is associative, we shall simplify expressions involving it by leaving out the parentheses used to indicate order of operation. We can justify this step by observing that no matter which order of operation is used, the same result is obtained. So we shall write $A \cap B \cap C$ for both $(A \cap B) \cap C$ and $A \cap (B \cap C)$.

Hence $$M(A, B, C) \bumpeq A \cap B \cap C,$$

and in future we shall use the latter notation to express the intersection of A, B, and C.

Example: We form $A \cap B \cap C$ by obtaining the lists for

$(A \cap B) \cap C$ and $A \cap (B \cap C)$.

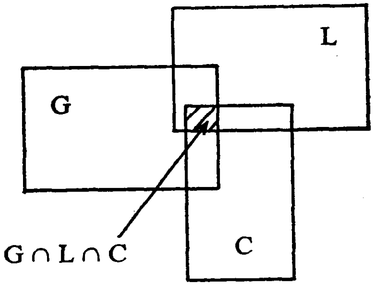
Using the lists on p. 22, we have:

$G \cap L$	$(G \cap L) \cap C$
Lucy	*Lucy*
Mary	*Mary*
Vera	*Vera*
Anne	

$L \cap C$	$G \cap (L \cap C)$
Lucy	*Lucy*
Mary	*Mary*
Vera	*Vera*
Bill	
Fred	
Jack	

Exercise 1. Using parentheses and the symbol $\cap$, write down all the possible expressions for the set $A \cap B \cap C$. (Remember that $\cap$ is both commutative and associative.)

If we seek a diagrammatic representation of $G \cap L \cap C$, we obviously have:



Exercise 2. Reproduce the above diagram, and mark regions corresponding to $G \cap L$, $G \cap C$, and $L \cap C$. What relation does $G \cap L \cap C$ bear to each of these subsets?

Exercise 3.

(i) Show that $A \cap A \bumpeq A$.

(ii) If $A \subseteq B$, show that $A \cap C \subseteq B \cap C$ for any subset C.

(iii) If $A \cap B \bumpeq U$, show that $A \bumpeq B \bumpeq U$.

Exercise 4. Work out ten of the possible different relationships between three subsets A, B, C of a set U, and for each draw an appropriate diagram. Verify that $A \cap B \cap C \bumpeq \emptyset$ is a possible result. What can be said of $A \cap B \cap C$ when one (at least) of A, B, C is $\emptyset$?

Exercise 5. We have given examples where parentheses have been used to denote the sequence of performing certain operations. Removal of parentheses was justified by observing that all possible sequences of performance yielded the same result. In our cases, we have also a simpler, 'observable' justification, namely that a sequence of operations was really another single operation. How would you explain, if asked, why

$$(3+2)+4 = 3+(2+4)?$$

Exercise 6. The fact that the intersection operation $\cap$ is associative means that order of operation is irrelevant in taking the intersection of any number of subsets. For example, to find the intersection of A, B, C and D is clearly the same as finding the intersection of (A and B) with (C and D), or of (A, B, and C) with D, etc., i.e.,

$$\begin{aligned}(A \cap B) \cap (C \cap D) &\bumpeq (A \cap B \cap C) \cap D \bumpeq \text{etc.}\\ &\bumpeq A \cap B \cap C \cap D.\end{aligned}$$

Use the associative law to show that $(A \cap B) \cap (C \cap D)$ and $A \cap (B \cap C) \cap D$ denote the same subset.

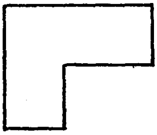
Exercise 7. Draw diagrams indicating $A \cap B$, $A \cap C$, $A \cap B \cap C$, and $(A \cap B) \cap (A \cap C)$. What do you infer? Explain your result in terms of lists.

2.3 *The union of two subsets*

We shall repeat the exposition of §§2.1, 2.2 (but more quickly) to discuss another method of subset formation. Beginning again with G and L, written in the form:

Anne Lucy *Mary Vera*	*Dorothy Evelyn Nancy* *Isobel Karen Olive* *Susan Una Yolande*
Bill Fred *Jack*	

we look not at the common part $\boxed{G \cap L}$, but at the totality of names, or the composite list represented above by the region:

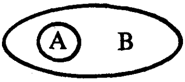


The names yielding this region are precisely the names of

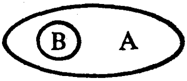
all the girls
all the left-handed children

and so determine a subset called the **union** of G and L, written as $G \cup L$. Clearly, this subset is determined by the pair G and L, and so $G \cup L \bumpeq L \cup G$. In other words, if we regard the process of forming the union of two subsets A, B as an operation on A, B, this operation is commutative: $A \cup B \bumpeq B \cup A$.

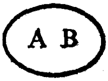
Thinking of all possible relations between two subsets A and B, we again reproduce the five diagrams:



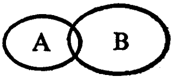
$A \subset B$

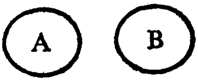


$B \subset A$



$A \bumpeq B$





as before. However, we have no difficulty with any of the possibilities here, since $A \cup B$ arises from combining the lists for A and B, and so is always given by a list; i.e., we need not introduce any 'new' subsets as we had to with the intersection operation.

Notice also that we are not concerned whether a given name appears on one list only or on both lists; in making out the list for $A \cup B$ we write each name once only, ensuring only that a given name has appeared in at least one of the lists for A and B. Thus 'an element belongs to $A \cup B$' means an element belongs either to A, or to B, or to both A and B. We shall use the single word 'or' as a connective to carry the above sense of 'either . . . or . . . or both' and so we have

Definition: If A, B are subsets of U, then the union of A and B, denoted by $A \cup B$, is defined as

$$A \cup B \bumpeq \{k : k \in A \text{ or } k \in B\}.$$

Exercise 8.

(i) Our definition of union leaves us in no doubt as to the meaning of $A \cup B$ if one of A, B is Ø. What about $Ø \cup Ø$?

(ii) What can be said of $A \cup B$ in the cases $A \subset B$, $B \subset A$, $A \bumpeq B$ respectively?

(iii) Is it possible that $A \cup B \bumpeq U$?

(iv) When does $A \cup B \bumpeq Ø$?

2.4 *Union of three subsets*

One way of finding the subset of children in the class who satisfy at least one of the requirements of

(a) being a girl, i.e., an element of G,

(b) being left-handed, i.e., an element of L,

(c) having a Christian name beginning with a consonant, i.e., an element of C, is simply to write down all three lists G, L, C as on page 22, and compile the list of all distinct names appearing at least once in the above lists. Hence we obtain the subset (using initial letter symbols)

$$\{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, Y\}$$

which we call the union of the subsets G, L, C, and write as $\bigcup(\mathrm{G, L, C})$. It is again clear that this subset is determined by the three sets G, L, C, and is independent of their arrangement, thus

$$\bigcup(\mathrm{G, L, C}) \bumpeq \bigcup(\mathrm{G, C, L}) \bumpeq \bigcup\,(\text{any arrangement of G, L, C}).$$

But we can achieve our purpose in the following way: combine the lists for G and L (thus producing $\mathrm{G} \cup \mathrm{L}$) and then combine this composite list with the list for C. Certainly, we finish with $\bigcup(\mathrm{G, L, C})$, but we took two steps instead of one: first we found $\mathrm{G} \cup \mathrm{L}$, then we found $(\mathrm{G} \cup \mathrm{L}) \cup \mathrm{C}$. So we conclude that

$$\bigcup(\mathrm{G, L, C}) \bumpeq (\mathrm{G} \cup \mathrm{L}) \cup \mathrm{C}$$

thus expressing the union of three sets in terms of the union-operation symbol $\cup$. Equally well, we could have first found $\mathrm{L} \cup \mathrm{C}$ and then $\mathrm{G} \cup (\mathrm{L} \cup \mathrm{C})$, again the required set. Thus

$$\mathrm{G} \cup (\mathrm{L} \cup \mathrm{C}) \bumpeq \bigcup(\mathrm{G, L, C}) \bumpeq (\mathrm{G} \cup \mathrm{L}) \cup \mathrm{C}.$$

In terms of the union operation $\cup$, this equation asserts that $\cup$ is again an associative operation, so that we may omit parentheses (whose function is to determine order of operation) in expressions such as $(\mathrm{A} \cup \mathrm{B}) \cup \mathrm{C}$, and write simply $\mathrm{A} \cup \mathrm{B} \cup \mathrm{C}$.

Exercise 9. Express $\mathrm{A} \cup \mathrm{B} \cup \mathrm{C}$ in the descriptive form

$$\{k : k \in (\qquad)\}.$$

Write out all possible ways of obtaining $\mathrm{A} \cup \mathrm{B} \cup \mathrm{C}$ as a result of two union operations, and draw diagrams indicating the subsets used with each operation.

Exercise 10.

(i) Show that $\mathrm{A} \cup \mathrm{A} \bumpeq \mathrm{A}$.
(ii) If $\mathrm{A} \subseteq \mathrm{B}$, show that $\mathrm{A} \cup \mathrm{C} \subseteq \mathrm{B} \cup \mathrm{C}$ for any subset C.
(iii) If $\mathrm{A} \cup \mathrm{B} \bumpeq \emptyset$, show that $\mathrm{A} \bumpeq \mathrm{B} \bumpeq \emptyset$.

Exercise 11. Show that $\mathrm{A} \cap \mathrm{B} \subseteq \mathrm{A} \cup \mathrm{B}$ for all A, B.

Exercise 12. The associativity of the union operation means that a 'symbol' such as $\mathrm{A} \cup \mathrm{B} \cup \mathrm{C} \cup \mathrm{D}$ may be used to denote any of the symbols obtainable from it by the insertion of parentheses, since all such symbols denote the same subset. Prove that

$$(A \cup B) \cup (C \cup D) \bumpeq A \cup (B \cup C) \cup D.$$

Exercise 13. By means of a diagram, investigate the relation between

$$A \cup B \cup C \text{ and } (A \cup B) \cup (A \cup C).$$

Use associative and commutative laws for $\cup$ to prove that

$$A \cup B \cup C \bumpeq (A \cup B) \cup (A \cup C).$$

Similarly prove that

$$A \cap B \cap C \bumpeq (A \cap B) \cap (A \cap C).$$

2.5 *The complement of a subset*

When we wrote down the list of names of girls in the class, the remaining names of course formed the list of boys in the class. Similarly, the children left after selection of all spectacle-wearers form a subset. In general, we call the subset formed by the remaining elements of U after the elements of a subset A have been removed the **complement** of A and denote it by $\tilde{A}$. The operation of taking the complement, or complementation, consists then of taking the subset of elements not belonging to the given subset. If the subset happens to be the whole basic set U, then clearly (since there are no elements remaining) we have $\tilde{U} \bumpeq \varnothing$. On the other hand, the complement of the null set must clearly be the whole set U, since $\varnothing$ has no elements; thus $\tilde{\varnothing} \bumpeq U$. What happens if we take the complement, $(\tilde{\tilde{A}})$, of $\tilde{A}$? Clearly, the elements not in $\tilde{A}$ are precisely the elements of A, and so we have $(\tilde{\tilde{A}}) \bumpeq A$. Similarly, $(\tilde{\tilde{U}}) \bumpeq \tilde{\varnothing} \bumpeq U$; $(\tilde{\tilde{\varnothing}}) \bumpeq \tilde{U} \bumpeq \varnothing$. [$(\tilde{\tilde{A}})$ is usually written simply as $\tilde{\tilde{A}}$.]

Exercise 14. (i) What is the subset formed by all elements which are not elements not belonging to G?

(ii) Show that $A \cup \tilde{A}$ and $A \cap \tilde{A}$ are each independent of the particular subset A.

(iii) If $A \subseteq B$, find $A \cap \tilde{B}$ and $\tilde{A} \cup B$.

2.6 *Subset formation involving the operations of union, intersection and complementation*

We wish to discuss some simple combinations of these operations, both as a means of forming subsets, and as a means of simplifying the naming of subsets.

(i) *Complementation of unions and intersections*

Given A, B, we form $A \cap B$ and look at its complement $\widetilde{(A \cap B)}$. Since the elements of $A \cap B$ are all elements of U belonging to both A and B, the remaining elements of U either do not belong to A (and so belong to $\tilde{A}$) or do not belong to B (and so belong to $\tilde{B}$). Therefore $\widetilde{(A \cap B)}$ is the subset of elements which belong to $\tilde{A}$ or to $\tilde{B}$, and so (by definition of union) is the subset $\tilde{A} \cup \tilde{B}$. Thus $\widetilde{(A \cap B)} \bumpeq \tilde{A} \cup \tilde{B}$. Similarly, the elements that do not belong to $A \cup B$ are all the elements which belong neither to A nor to B; hence they are precisely the elements belonging to both $\tilde{A}$ and $\tilde{B}$, and so form $\tilde{A} \cap \tilde{B}$. Thus $\widetilde{(A \cup B)} \bumpeq \tilde{A} \cap \tilde{B}$.

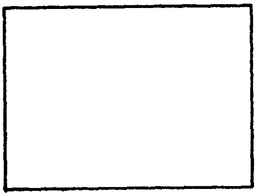
Here, we add a note on method. If we wish to show that two subsets A, B are identical, i.e., that $A \bumpeq B$, often the most convenient way is to verify both of the relations $A \subseteq B$, $B \subseteq A$; for then $A \bumpeq B$ (by comparing lists of elements). For example, to prove that $\widetilde{(A \cup B)} \bumpeq \tilde{A} \cap \tilde{B}$, we have

(a) If $k \in \widetilde{(A \cup B)}$, then $k \notin A \cup B$. So $k \notin A$ and $k \notin B$; i.e., $k \in \tilde{A}$ and $k \in \tilde{B}$. Hence $k \in \tilde{A} \cap \tilde{B}$.

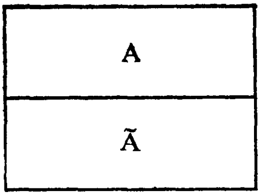
(b) If $k \in \tilde{A} \cap \tilde{B}$, then $k \in \tilde{A}$ and $k \in \tilde{B}$. So $k \notin A$ and $k \notin B$, whence $k \notin A \cup B$. Thus $k \in \widetilde{(A \cup B)}$.

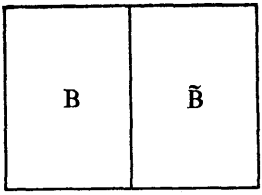
(a) shows $\widetilde{(A \cup B)} \subseteq \tilde{A} \cap \tilde{B}$, (b) shows $\tilde{A} \cap \tilde{B} \subseteq \widetilde{(A \cup B)}$, hence $\widetilde{(A \cup B)} \bumpeq \tilde{A} \cap \tilde{B}$.

Use of a diagram: We shall for convenience consistently regard U as represented by a large square or rectangle, usually unlabelled:

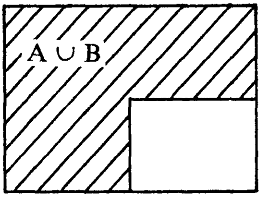


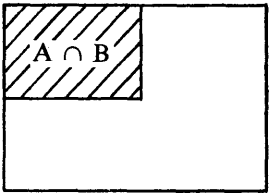
A typical subset A will be represented by the upper half (and consequently $\tilde{A}$ by the lower half), while we shall use the left half to represent a second subset, say B:



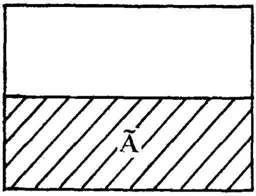


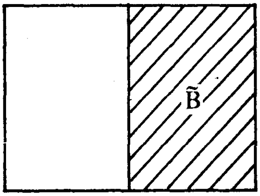
(We remind our readers that shape and size of regions on our diagrams are not significant, and suggest that all our diagrams be redrawn freely.) Regions corresponding to $A \cup B$ and $A \cap B$ will clearly be:

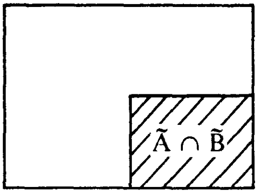


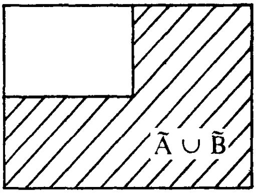


while the unshaded regions are respectively $(\widetilde{A \cup B})$ and $(\widetilde{A \cap B})$. But, looking at $\tilde{A}$ and $\tilde{B}$, and forming $\tilde{A} \cap \tilde{B}$ and $\tilde{A} \cup \tilde{B}$, we have:





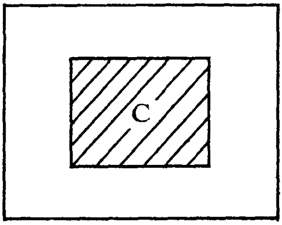




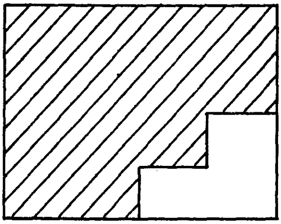
and here on comparing diagrams we have the two recently established identities. Moreover, the construction process on the diagrams indicates the thought-processes necessary to prove these identities. *Exercise* 15. You may argue that A and B need not intersect as shown. Draw pairs of diagrams showing all possible relations between the regions for A and B, and for each pair reproduce the eight diagrams obtained above, comparing the relevant regions as we have done above.

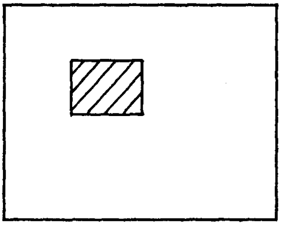
(ii) *Examples involving three subsets A, B, C*

We have already met $A \cup B \cup C$ and $A \cap B \cap C$, where in each case we have observed that the arrangement of the letters A, B, C, and the insertion of parentheses [as e.g. $(A \cap B) \cap C$] is irrelevant. These subsets corresponded respectively to the combined lists of elements in A, B, C and the list of elements common to A, B, C. If we denote C on our basic diagram by the region shaded below:



we have the diagrams:





for $A \cup B \cup C$ and $A \cap B \cap C$ respectively.

Suppose we wish to construct the subset whose elements belong not only to A, but also to either B or C. If we call this subset F, we have

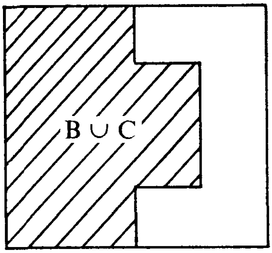
$$F \bumpeq \{k : k \in A \text{ and } k \in (B \text{ or } C)\}.$$

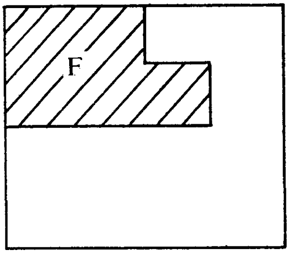
But '$k \in (B$ or $C)$' is properly written as '$k \in B \cup C$' for this is precisely what $k \in B \cup C$ means. Hence we have

$$F \bumpeq \{k : k \in A \text{ and } k \in B \cup C\}.$$

But we recognise the condition on our element k; it says precisely that k belongs to the intersection of A and $B \cup C$. Thus F is simply

$A \cap (B \cup C)$. Notice the significance of parentheses here. First, we form the union $B \cup C$. Then we take its intersection with A. In diagrams:





Exercise 16. (i) Describe the set of children who are boys and either left-handed or spectacle-wearers in terms of B, L, S, $\cap$ and $\cup$.

(ii) Does $A \cap (C \cup B) \bumpeq A \cap (B \cup C)$? Why?

(iii) Draw diagrams illustrating $A \cap (B \cup C)$ in the cases when $B \subset C$, $B \subset A$ respectively. Can you find examples of each of these using the subsets of the children in the class?

Now let us construct the subset H for instance, whose elements belong either to C or to both A and B; i.e.,

$$H \bumpeq \{k : k \in C \text{ or } k \in (A \text{ and } B)\}.$$

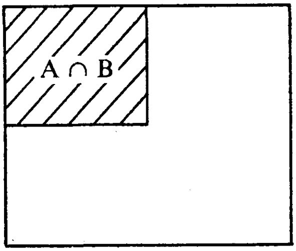
'$k \in (A \text{ and } B)$' is properly written as '$k \in A \cap B$' (why?) and so $H \bumpeq \{k : k \in C \text{ or } k \in A \cap B\}$. This is again a familiar form, for it says that H is the union of C and $A \cap B$, thus

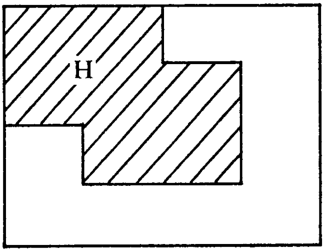
$$H \bumpeq C \cup (A \cap B)$$

(notice again the use of parentheses to specify the sequence of operations), which, because $\cup$ is a commutative operation, gives

$$H \bumpeq (A \cap B) \cup C.$$

Using diagrams, we have:





Exercise 17. (i) Describe the set of children who either wear spectacles or are left-handed boys in terms of B, L, S, $\cap$ and $\cup$.

(ii) Is $(A \cap B) \cup C \bumpeq (B \cap A) \cup C$? Why?

(iii) Draw diagrams illustrating $(A \cap B) \cup C$ in the cases when $A \subset B$, $A \subset C$ respectively. Can you find examples of each of these among the subsets of the children in the class?

One glance at the diagrams convinces us that F and H are not always equal, i.e., in general,

$$(A \cap B) \cup C \not\bumpeq A \cap (B \cup C),$$

and indeed there is no reason why they should be equal, since their manners of formation are quite different. But the two sets F, H are determined symbolically in terms of A, B, C, $\cap$, and $\cup$ precisely by the position of the parentheses, otherwise their symbols are identical. Therefore, we cannot omit the parentheses and write simply $A \cap B \cup C$, since for this symbol to have meaning, all possible choices for the order of performing the operations $\cap$ and $\cup$ must yield the same subset, and we have just seen that this is not so. Remember that meaning could be given to $A \cap B \cap C$ because we could construct a single operation (combining all three lists) to replace the pairs of operations of combining lists two at a time, and similarly for $A \cup B \cup C$. We cannot do this for the symbol $A \cap B \cup C$; it does not correspond to any single process on the elements of A, B, C.

Summing up, we make three points clear:

1. If we describe a process of subset formation in words, our description specifies an order of operation which must be preserved symbolically by the correct use of parentheses. Thus we have subsets of the form $(A \cap B) \cup C$, $A \cap (B \cup C)$, etc.

2. 'Symbols' such as $A \cap B \cup C$, which are in themselves meaningless, cannot be made meaningful because different attempts to make them meaningful (by insertion of parentheses) produce different meanings, while for us, a symbol must always have a clear unambiguous meaning.

3. If we remember always that our symbolic language is representing lists, relations between them and operations on them, and if we argue first with lists and finally express our results symbolically, we should never produce 'symbols' such as $A \cap B \cup C$, and we should not even be tempted to suppose $A \cap (B \cup C)$ and $(A \cap B) \cup C$

were the same set simply because symbolically, they 'looked rather similar'. Danger arises when we try to argue in symbols, forgetting their meanings. That can only be done when we have trained ourselves to think in symbols, i.e., to justify mentally each manipulation of a symbolic expression.

Exercise 18. We have $(\widetilde{A \cup B}) \bumpeq \tilde{A} \cap \tilde{B}$, $(\widetilde{A \cap B}) \bumpeq \tilde{A} \cup \tilde{B}$. Can you express the complement of $A \cup B \cup C$ and of $A \cap B \cap C$ in terms of $\tilde{A}$, $\tilde{B}$, $\tilde{C}$?

By drawing a series of diagrams, work out the steps of a proof. Also give proofs using the $A \subseteq B$, $B \subseteq A$ technique explained earlier.

Exercise 19. Express $(\widetilde{A \cap B}) \cup C$, $A \cap (\widetilde{B \cup C})$, $(\widetilde{(A \cap B) \cup C})$, $\widetilde{(A \cap (B \cup C))}$ in terms of A, B, C and their complements. Are any two of these sets identical?

Exercise 20. If $A \subset B$, what relation exists between $\tilde{A}$ and $\tilde{B}$? If $A \subset B \subset C$, what relations exist between $\tilde{A}$, $\tilde{B}$ and $\tilde{C}$?

(iii) *Simplifying the symbol for a subset*

We have identities such as $A \cap A \bumpeq A$, $A \cup A \bumpeq A$, $A \cap \tilde{A} \bumpeq \emptyset$, $A \cup \tilde{A} \bumpeq U$, which enable us to replace one symbol by a simpler one, a process which corresponds to replacing a description of a subset by a shorter description, e.g.,

$$\begin{aligned} A \cap A &\bumpeq \{k : k \in A \text{ and } k \in A\} \\ &\bumpeq \{k : k \in A\} \\ &\bumpeq A. \end{aligned}$$

Suppose we wished to list the children in U who were either girls and left-handed or girls with names beginning with a consonant. According to the description, the list we want is given precisely by the symbol $(G \cap L) \cup (G \cap C)$, i.e. {girls and left-handed} or {girls with names beginning with a consonant}. But we can simplify the description to yield 'girls who either are left-handed or have a name beginning with a consonant', which is given symbolically by $G \cap (L \cup C)$ (why?). Since we have the same list in both cases, we conclude that

$$(G \cap L) \cup (G \cap C) \bumpeq G \cap (L \cup C).$$

Using the commutative laws already found, we obtain

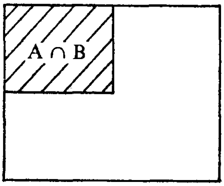
$$(L \cap G) \cup (C \cap G) \bumpeq (L \cup C) \cap G.$$

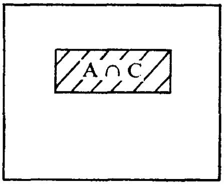
(How many times did we apply the commutative laws?)

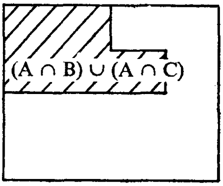
In general, we conclude that for any subsets A, B, C, of U

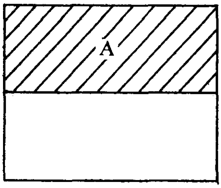
$$(A \cap B) \cup (A \cap C) \bumpeq A \cap (B \cup C),$$
$$(B \cap A) \cup (C \cap A) \bumpeq (B \cup C) \cap A.$$

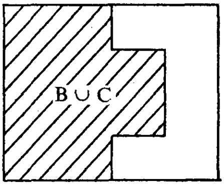
A property of this type is called **distributive.** It expresses a property of the two operations ∩ and ∪ which in words is: 'Taking the union of subsets each of which is an intersection involving a particular subset, A, for instance, is the same as taking the intersection with A of the union of all the other subsets involved'. On a diagram, we can see the different processes leading to the same subset:

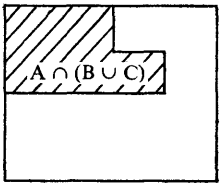












In the first set of diagrams, intersection operations preceded the union operation. This order is reversed in the second set. (The law $a(b+c) = ab+ac$ in ordinary arithmetic asserts the validity of a similar interchange of order of operations.)

Exercise 21. Find a simpler description meaning the same as 'children who are *both* girls or left-handed *and* girls or have a name beginning with a consonant'.

Deduce the identities

$$(A \cup B) \cap (A \cup C) \bumpeq A \cup (B \cap C)$$
$$(B \cup A) \cap (C \cup A) \bumpeq (B \cap C) \cup A$$

for any subsets A, B, C of U.

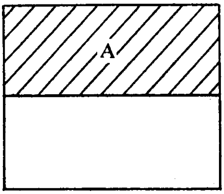
Draw diagrams illustrating the different methods of formation given by each side of one of the above identities.

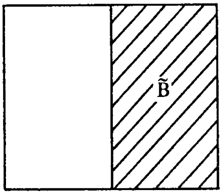
Exercise 22. Sometimes an analogy is drawn between $\cup$ and $+$, $\cap$ and $\times$, where $+$ and $\times$ are the ordinary arithmetical operations. By considering the meaning of $A \cap A$, $A \cup A$, and both the distributive laws just obtained, one can see that the analogy, although suggestive, is not entirely satisfactory.

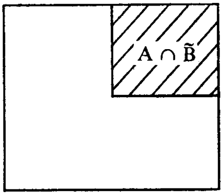
Exercise 23. Simplify $A \cap (B \cup \tilde{A})$, $A \cup (A \cap B)$, $A \cup (B \cap \tilde{B})$, $A \cup (B \cap U)$, $(A \cup B) \cap (A \cup \tilde{B})$.

2.7 *Two further operations on subsets*

Let A, B be any two subsets of a set U. What is the set of elements which belong to A but not to B? (e.g., which girls in the class are not left-handed?) If we call the required subset K, then since all its elements must belong to A, K is a subset of A, so $K \subseteq A$. Since no element of K can belong to B, every element of K belongs to $\tilde{B}$, so $K \subseteq \tilde{B}$. We see in fact that K consists precisely of the elements of U which belong to A and $\tilde{B}$, and so K is the intersection $A \cap \tilde{B}$ of A and the complement of B. On our diagram we have:

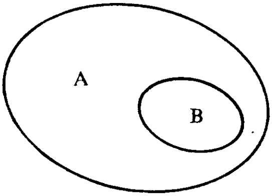


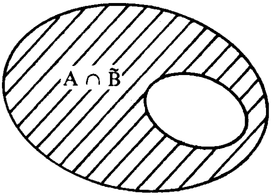




Thus $A \cap \tilde{B} \bumpeq \{k : k \in A \text{ and } k \notin B\}$.

Suppose now we consider the special case when B is a subset of A, $B \subseteq A$. Then $A \cap \tilde{B}$ has the following interpretation: it consists precisely of the elements of A which are not elements of B. A diagram makes this self-evident:





Thus, when $B \subseteq A$, the list of elements of $A \cap \tilde{B}$ is obtained by removing the list for B from the list for A, or 'taking away the B-list from the A-list'.

It seems natural now to write the subset K symbolically in the form $A-B$, indicating its manner of formation. We therefore define a new operation, which we shall call not 'subtraction', but **'set-difference'** or (recalling the original idea of $A \cap \tilde{B}$) **'relative complementation'**.

Definitions: If $B \subseteq A$, then the set-difference of B with respect to A, denoted by $A-B$ and read usually as 'A minus B'is the subset

$$A-B \bumpeq \{k : k \in A \text{ but } k \notin B\}.$$

For any two subsets A, B, the relative complement of B with respect to A is the intersection $A \cap \tilde{B}$ of A and the complement of B. In the special case $B \subseteq A$, we have

$$A-B \bumpeq A \cap \tilde{B}$$

and this relation is used to define the set-difference of any two subsets A and B.

Exercise 24. Can $\tilde{A}$ be expressed in a form involving the operation '$-$'?

Exercise 25. (i) Show that $A-A \bumpeq \emptyset$.

(ii) If $A-B \bumpeq \emptyset$, prove that $A \subseteq B$.

Exercise 26. Find the elements of each of the subsets $L-S$, $S-V$, $V-S$, $(G-V)-S$, and $G-(V-S)$ of the set of children.

Exercise 27. Is set-difference a commutative operation; i.e., is it true that for all subsets A, B of a set U, $A-B \bumpeq B-A$?

Exercise 28. Is set-difference an associative operation; i.e., is it true that for all subsets A, B, C of a set U

$$A-(B-C) \bumpeq (A-B)-C?$$

Exercise 29. Verify that, if $B \subseteq A$, $A-(A-B) \bumpeq B$.

Exercise 30. Can parentheses be omitted from the expression $A-(A-B)$?

Exercise 31. Find expressions for $A-(B \cup C)$ and $A-(B \cap C)$ in terms of $A-B$ and $B-C$.

Exercise 32. Investigate whether either of $\cap$ or $\cup$ is distributive over $-$ i.e., is either of the relations

$$A \cap (B-C) \bumpeq (A \cap B)-(A \cap C),$$
$$A \cup (B-C) \bumpeq (A \cup B)-(A \cup C)$$

true for all subsets A, B, C of a set U?

We now look at the complement $\tilde{K}$ of the set $K \bumpeq A \cap \tilde{B}$. By the rules already established,

$$\tilde{K} \bumpeq \widetilde{(A \cap \tilde{B})}$$

$$\bumpeq \tilde{A} \cup \tilde{\tilde{B}}$$

(complement of intersection is the union of complements)

$$\bumpeq \tilde{A} \cup B$$

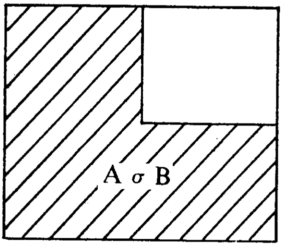
(complement of a complement yields original subset).

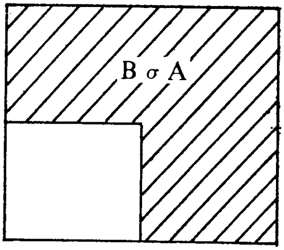
Thus $\tilde{K} \bumpeq \{k : k \notin A \text{ or } k \in B\}$. We define an operation which we shall call 'sigma', denoted by σ, as follows:

For any two subsets A, B of U,

$$A \,\sigma\, B \overset{\text{def}}{\bumpeq} \tilde{A} \cup B.$$

Let us find its properties. Firstly, does it matter whether we write $A \,\sigma\, B$ or $B \,\sigma\, A$? [i.e., is the σ-operation commutative?] We draw diagrams:





and see that the answer is 'Yes; it does matter whether we write $A \,\sigma\, B$ or $B \,\sigma\, A$'.

Thus σ is not commutative, and we must take care that we use the correct symbol, $A \,\sigma\, B$ or $B \,\sigma\, A$, when we mean one of these subsets.

Perhaps there are special subsets A, B of U for which the relation $A \,\sigma\, B \bumpeq B \,\sigma\, A$ is true. Let us investigate. If so, we have

$$\tilde{A} \cup B \bumpeq \tilde{B} \cup A. \tag{1}$$

Now $\tilde{B} \cup A$ is the complement of $(\tilde{A} \cap B)$, so we have

$$\tilde{A} \cup B \bumpeq \widetilde{(\tilde{A} \cap B)}. \tag{2}$$

But $\tilde{A} \cap B$ is a subset of $\tilde{A} \cup B$, $\tilde{A} \cap B \subseteq \tilde{A} \cup B$. Hence, by (2)

$$\tilde{A} \cap B \subseteq \widetilde{(\tilde{A} \cap B)}. \tag{3}$$

Write $X \bumpeq \tilde{A} \cap B$. Then (3) says $X \subseteq \tilde{X}$. But a set and its complement are disjoint, i.e., they have no elements in common. This contradicts (3) unless $X \bumpeq \varnothing$, for then we can satisfy both the statements $X \cap \tilde{X} \bumpeq \varnothing$, $X \subseteq \tilde{X}$. We deduce

$$(4) \qquad \tilde{A} \cap B \bumpeq \varnothing \text{ and } \widetilde{(\tilde{A} \cap B)} \bumpeq A \cup \tilde{B} \bumpeq U.$$

Similarly, using (1) but observing that

$$\tilde{A} \cup B \bumpeq \widetilde{(A \cap \tilde{B})},$$

we deduce

$$(5) \qquad A \cap \tilde{B} \bumpeq \varnothing \text{ and } \tilde{A} \cup B \bumpeq U.$$

(4) and (5) can be rewritten as

$$(6) \qquad \tilde{A} \cap B \bumpeq \varnothing,\ \tilde{A} \cup B \bumpeq U,$$

$$(7) \qquad \tilde{B} \cap A \bumpeq \varnothing,\ \tilde{B} \cup A \bumpeq U.$$

(6) expresses the relationship which determines the complement $\tilde{B}$ of B:

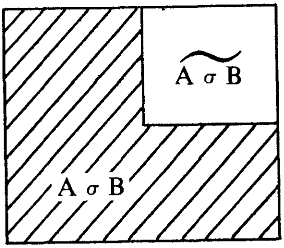
$$\tilde{B} \cap B \bumpeq \varnothing,\ \tilde{B} \cup B \bumpeq U,$$

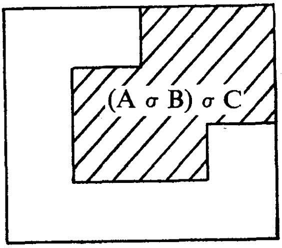
so

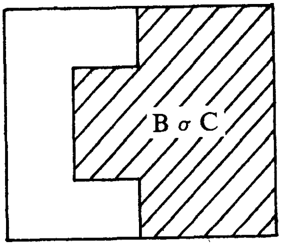
$$\tilde{A} \bumpeq \tilde{B}, \text{ i.e., } A \bumpeq B.$$

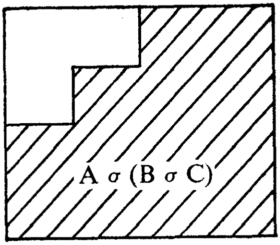
(7) says the same thing, $A \bumpeq B$. Thus we have discovered that $A \,\sigma\, B \bumpeq B \,\sigma\, A$ only when $B \bumpeq A$, then $A \,\sigma\, A \bumpeq \tilde{A} \cup A \bumpeq U$.

Next, we examine $(A \,\sigma\, B) \,\sigma\, C$ and $A \,\sigma\, (B \,\sigma\, C)$ to see whether order of operation is important, i.e., whether parentheses may be omitted, i.e., whether σ is associative. We draw diagrams:









and conclude that again the answer is 'no', so parentheses must be preserved in using σ.

Exercise 33. Express $A \sigma (B \sigma C)$ and $(A \sigma B) \sigma C$ in terms of $\cup$, $\cap$ and $\tilde{}$. Verify that

$$(A \sigma B) \sigma C \subseteq A \sigma (B \sigma C).$$

In which of the following cases can the $\subseteq$ above always be replaced by $\bumpeq$?

(a) $A \subseteq \tilde{C}, B \subseteq \tilde{C}$,
(b) $A \subset B$,
(c) $A \cap \tilde{B} \subseteq C$.

Exercise 34. Show that $(A-B) \sigma A$ is independent of the subsets A, B.

Exercise 35. Show that $A \sigma (B-A)$ is independent of the subset B.

Exercise 36. Simplify $(A \cup B) \sigma C$, $A \sigma (B \cup C)$, $(A \cap B) \sigma C$, $A \sigma (B \cap C)$, $A \sigma \tilde{A}$.

Exercise 37. Show that $(A \sigma B) \cap (B \sigma C) \subseteq A \sigma C$.

2.8 *Primary subsets of a set*

Given a set U, and different descriptions determining subsets A, B, C, . . . (and their complements $\tilde{A}$, $\tilde{B}$, $\tilde{C}$, . . .), we shall call a subset of U a **primary subset** if it consists of all elements which have identical descriptions in terms of the descriptions used to determine A, B, C, ... Some examples will clarify this definition.

Given one description on U, determining say A, the primary subsets will be A and $\tilde{A}$, since the elements of U either satisfy or do not satisfy the given description.

Given two descriptions on U, determining say A, B, we argue as follows. The elements of A can be distinguished according to their satisfying the description determining B, or not. So we have $A \cap B$ and $A \cap \tilde{B}$. Similarly, from $\tilde{A}$, we produce $\tilde{A} \cap B$ and $\tilde{A} \cap \tilde{B}$. This exhausts all the possibilities in terms of two descriptions; thus the primary subsets are the four subsets $A \cap B$, $\tilde{A} \cap B$, $A \cap \tilde{B}$, $\tilde{A} \cap \tilde{B}$.

Similarly, if three descriptions are given, specifying A, B, C respectively, the primary subsets will consist of the eight subsets

$$A \cap B \cap C, \tilde{A} \cap B \cap C, A \cap \tilde{B} \cap C, \tilde{A} \cap \tilde{B} \cap C,$$
$$A \cap B \cap \tilde{C}, A \cap \tilde{B} \cap \tilde{C}, \tilde{A} \cap B \cap \tilde{C}, \tilde{A} \cap \tilde{B} \cap \tilde{C}.$$

Exercise 38. If we are given n descriptions determining n subsets, how many primary subsets will there be?

Exercise 39. In terms of the class U and its subsets G, L, S, C, determine all the distinct primary subsets. Notice that in a particular example, it may easily happen that some primary subsets have no elements.

Exercise 40. From n initial subsets, the primary subsets are formed as in Exercise 38. If we now form all possible unions of any number of primary subsets, show that the number of subsets thus produced is 2^{2^n}. (See the example below.) Are they necessarily all distinct?

Example: Given two subsets A, B, of U, we have seen that there are four primary subsets, viz., $A \cap B$, $\tilde{A} \cap B$, $A \cap \tilde{B}$, $\tilde{A} \cap \tilde{B}$:

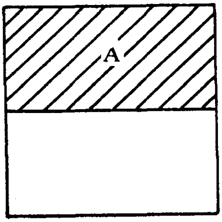
$A \cap B$	$A \cap \tilde{B}$
$\tilde{A} \cap B$	$\tilde{A} \cap \tilde{B}$

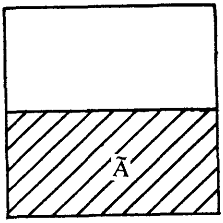
We now form all possible unions.

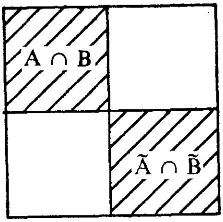
(a) Using none gives Ø, the empty set.

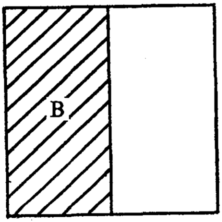
(b) Using one gives the four primary subsets.

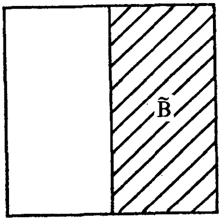
(c) Using two, gives:

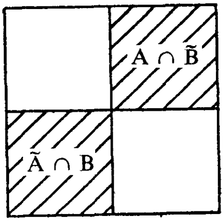




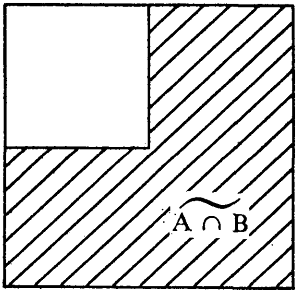


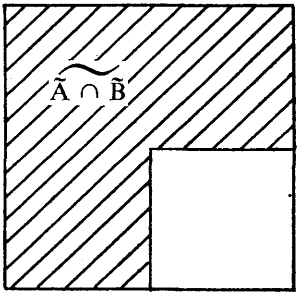


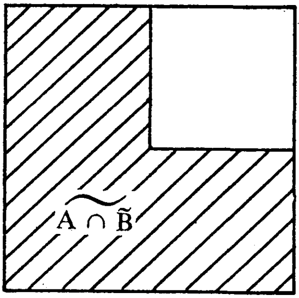


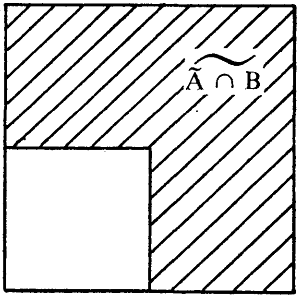


(d) Using three gives the four complements of primary subsets :









(e) Using all four gives U.

There are thus $1+4+6+4+1 = 2^4$ subsets produced by unions of primary subsets corresponding to two initial subsets.

2.9 *Duality*

If we examine all the results we have so far derived, we discover a remarkable fact. Consider, for example, the following pairs of relations among subsets A, B, C of U.

$$\begin{aligned}
A \cap B &\overset{\frown}{=} B \cap A &\quad\text{and}\quad& A \cup B \overset{\frown}{=} B \cup A\\
(A \cap B) \cap C &\overset{\frown}{=} A \cap (B \cap C) &\quad\text{and}\quad& (A \cup B) \cup C \overset{\frown}{=} A \cup (B \cup C)\\
A \cap \emptyset &\overset{\frown}{=} \emptyset &\quad\text{and}\quad& A \cup U \overset{\frown}{=} U\\
A \cap U &\overset{\frown}{=} A &\quad\text{and}\quad& A \cup \emptyset \overset{\frown}{=} A
\end{aligned}$$

In the first two cases, each relation is obtained from the other by interchanging $\cap$ and $\cup$. In the others, we also interchange Ø and U.

These ideas suggest the truth of the following result: If we have derived a relation involving subsets of U, and if we interchange $\cap$ and $\cup$; Ø and U, then the relation thus obtained may also be derived by us. For example, from

$$A \cap \tilde{A} \bumpeq \emptyset \qquad \text{we have} \qquad A \cup \tilde{A} \bumpeq U$$

$$\widetilde{(A \cap B)} \bumpeq \tilde{A} \cup \tilde{B} \quad \text{we have} \quad \widetilde{(A \cup B)} \bumpeq \tilde{A} \cap \tilde{B},$$

results which have been obtained previously.

The result given above is called a **duality principle.** It asserts that given a certain result, its **dual** (obtained by carrying out the appropriate interchanges) is a result that can also be obtained by a direct argument.

Exercise 41. We know that if $A \subseteq B$, then $A \cap B \bumpeq A$ and $A \cup B \bumpeq B$. Can you suggest an extension of our duality idea to the symbols $\subseteq$, $\supseteq$ by comparing these results with some previously obtained?

2.10 *Summary. Formulation of a mathematical system*

By the process of patiently building up various lists (subsets) composed of those objects (elements) in an initial list (universal set) which satisfy certain descriptions, we have developed several operations on subsets, namely intersection, union, complementation (and some others), and introduced several types of symbols to simplify our explanations and to help us in thinking out our way. In fact, we have acquired a reasonable collection of information on the methods of forming subsets of a set (i.e., on the construction of sorting processes). Putting our information down in symbols gives us a handy compendium containing properties of various operations and knowledge expressed by certain relations. If we include in our 'ready reference' a description of the symbols we have introduced, we have a synopsis of all the preceding work. Presumably, anyone with a quick mind and an ability to digest brief statements could be content with the following account.

Definitions: A set is a clearly defined collection of distinguishable objects. In the sequel, a given universal or basic set will be denoted by the symbol U. The objects forming U will be denoted by small letters $a, b, c, \ldots$. The symbol k will be used in referring to an arbitrary element of U. U will also be denoted by the symbol $\{a, b, \ldots\}$, where within the braces the symbols for the elements of U are each written once and once only. '$k \in U$' denotes the sentence 'k is an element of U'.

A subset of U is any part of the collection forming U. Subsets will be denoted by capital letters A, B, C, ... They are also denoted as $\{a, \ldots .\}$, where within the braces are written once and once only the symbols for the elements of the subset. Subsets and (basic) sets are also denoted by a symbol of the form

$$\{k : k \text{ satisfies a certain description}\}$$

where the corresponding subset consists of all elements which satisfy the description specified.

When two subsets have the same elements, they are (regarded as) the same set. The symbol '$\triangleq$' denotes the phrase 'is the same set as', thus $A \triangleq B$ says 'A is the same set as B'.

All the elements of a subset of U are elements of U. Sometimes all elements of one subset, say A, are elements of another subset, say B. Then A is said to be contained in B, and this relation is denoted by the symbol '$\subseteq$', thus $A \subseteq B$. If there are elements of B not belonging to A, A is called a proper subset of B, and we write $A \subset B$. Similarly, '$\supseteq$' and '$\supset$' are used for 'contains' and 'properly contains' respectively.

Operations: If A, B are arbitrary subsets of U, then

(a) their union $A \cup B$ is the subset

$$A \cup B \triangleq \{k : k \text{ belongs either to A, or to B, or to both}\}$$

written as

$$A \cup B \triangleq \{k : k \in A \text{ or } k \in B\};$$

(b) their intersection $A \cap B$ is the subset

$$A \cap B \triangleq \{k : k \text{ belongs to both A and B}\}$$

written as

$$A \cap B \triangleq \{k : k \in A \text{ and } k \in B\};$$

(c) the complement $\tilde{A}$ of A is the subset

$$\tilde{A} \triangleq \{k : k \in U \text{ and } k \notin A\}.$$

Finally, the symbol $\varnothing$ denotes the null set, the subset with no elements. It is given the special property $\varnothing \subseteq A$ for all subsets A of U.

Then, from the definition, the previously obtained commutative, associative and distributive properties of $\cap$ and $\cup$ are established, together with the properties of complementation. Other operations $(-, \sigma)$ are defined and their properties explored. The following 'ready reference' tables these results:

1. $\varnothing \overset{\text{def}}{\triangleq}$ the null set $\triangleq$ the set with no elements.

For any $A \subseteq U$, $\varnothing \subseteq A$.

2. $A \cap B \overset{\text{def}}{\bumpeq} \{k : k \in A \text{ and } k \in B\}$. (intersection of A and B)

$A \cap B \bumpeq B \cap A$. (commutative property)

$A \cap (B \cap C) \bumpeq (A \cap B) \cap C$ (associative property)

$\overset{\text{def}}{\bumpeq} A \cap B \cap C$.

3. $A \cup B \overset{\text{def}}{\bumpeq} \{k : k \in A \text{ or } k \in B\}$. (union of A and B)

$A \cup B \bumpeq B \cup A$. (commutative property)

$A \cup (B \cup C) \bumpeq (A \cup B) \cup C$ (associative property)

$\overset{\text{def}}{\bumpeq} A \cup B \cup C$.

4. $A \cap (B \cup C) \bumpeq (A \cap B) \cup (A \cap C)$.

$A \cup (B \cap C) \bumpeq (A \cup B) \cap (A \cup C)$. (distributive properties of $\cap$ and $\cup$)

5. $\tilde{A} \overset{\text{def}}{\bumpeq} \{k : k \in U \text{ and } k \notin A\}$. (complement of A)

$(\tilde{\tilde{A}}) \bumpeq A$.

$(\widetilde{A \cap B}) \bumpeq \tilde{A} \cup \tilde{B}$.

$(\widetilde{A \cup B}) \bumpeq \tilde{A} \cap \tilde{B}$.

$A \cap \tilde{A} \bumpeq \emptyset, \; A \cup \tilde{A} \bumpeq U$.

6. If $B \subseteq A$, $A - B \overset{\text{def}}{\bumpeq} \{k : k \in A \text{ and } k \notin B\}$. (set-difference)

$A - B \bumpeq A \cap \tilde{B}$.

For any A, B, $A \cap \tilde{B}$ (the complement of B relative to A) is called the set-difference and written $A - B$.

7. $A \,\sigma\, B \overset{\text{def}}{\bumpeq} \tilde{A} \cup B \bumpeq (\widetilde{A \cap \tilde{B}})$

$\bumpeq$ complement of the set-difference $A - B$.

Note: Except in the last chapter, the book deals exclusively in sets whose members can be listed, i.e., in 'finite' sets. The whole subject of sets only some of whose members can be listed, while others are described only by an iterative rule, is deferred to the last chapter. Many, in fact most, of the results which are obtained for the finite sets are however valid for sets whose members can only be described in this way.

Chapter 3

DESCRIPTIONS AND STATEMENTS

3.1 *Introduction*

We are now going to apply notions developed earlier to a new purpose—an investigation of the form of descriptive statements.

First, let us recall the method of production of subsets from the list of children in a class. We distinguished those children who satisfied a certain description; for example,

$$\mathrm{L} \doteqdot \{A, B, F, J, L, M, V\}$$

denoted the set of children who were left-handed. We also agreed to describe L as

$$\mathrm{L} \doteqdot \{k : k \text{ is a child who is left-handed}\}$$

where the meaning of the sentence in braces is 'all children in the class who satisfy the requirement that they are left-handed'.

Generally speaking, all our subsets were derived by making a statement or proposition of the form 'This is a child who satisfies a certain condition' (e.g., 'This is a child who is a girl') and listing only those children who satisfied that condition—i.e., only those children for whom the description was a true description. Notice that for each of our conditions, we could always decide whether it was satisfied or not satisfied by each of the children in the class.

Such a description (which, when applied to the objects of a given collection, is found to give either a correct or an incorrect description of each one) is called a **statement**. We are going to show how an understanding of various relations between subsets leads to an understanding of relations between statements. That is, we shall use our examples of operations and relations on sets to build up a 'statement language'.

3.2 *The negation of a statement*

We introduce some symbols in order to simplify our argument Instead of writingT his is a child who satisfies a certain (unspecified) condition', we shall simply write p, and refer to the statement p.

Other symbols used to denote general statements will be the letters q, r, s. When we wish to refer to a particular statement, we shall give it a distinctive symbol, e.g., 'This is a child who is a girl' might be denoted by p_G: 'This is a child who is left-handed' by p_L, etc.

Our first remark will be this, then. A statement p applicable to a set U determines a subset, P, say, by the rule

$$\mathrm{P} \doteqdot \{k : k \in \mathrm{U}, k \text{ satisfies } p\}.$$

We have the examples

$$\mathrm{G} \doteqdot \{k : k \text{ satisfies } p_G\},$$

$$\mathrm{L} \doteqdot \{k : k \text{ satisfies } p_L\},$$

and $$\mathrm{B} \doteqdot \{k : k \text{ satisfies } p_B\}$$

where p_B is the statement 'This is a child who is a boy'.

We fix our attention on the statements p_G and p_B, with the corresponding subsets G and B. Clearly any child who does not belong to G must belong to B, i.e., G and B are complementary subsets of U. We have already a notation for this idea; we write $\mathrm{B} \doteqdot \tilde{\mathrm{G}}$, $\mathrm{G} \doteqdot \tilde{\mathrm{B}}$. What can be said about the statements p_G and p_B? Clearly any child who satisfies the statement p_G does not satisfy p_B, and vice versa. We can make this remark self-evident by observing that p_B can be written in the form 'This is a child who is not a girl', and p_G in the form 'This is a child who is not a boy'.

In other words, the descriptive condition contained in the statement p_G is the negation of that condition contained in the statement p_B.

This happens often when dealing with statements; so often that a symbol has been invented to denote the negation or denial of a given statement. The negation, 'not-p' is denoted by '$\sim p$'. For example $\sim p_G$ means the statement 'This is a child who is not a girl', and so is the same statement as 'This is a child who is a boy'.

Thus if, when discussing statements, we use the symbol $\doteqdot$ to mean 'is the same statement as' we may write

$$\sim p_G \doteqdot p_B,$$

and similarly

$$\sim p_B \doteqdot p_G.$$

Notice the correspondence with the relation

$$\tilde{\mathrm{G}} \doteqdot \mathrm{B}$$

and $$\tilde{\mathrm{B}} \doteqdot \mathrm{G}.$$

Exercise 1. Express the other subsets of U in the form of statements $\{k : k$ satisfies the statement $p\}$. By listing pairs of complementary sets, find as many negations '$\sim p$' as possible.
Draw up a table:

Subset	Complement	Statement p	$\sim p$
G	$B \mathrel{\hat{=}} \tilde{G}$	p_G	$\sim p_G \mathrel{\hat{=}} p_B$

3.3 *Conjunction and disjunction of statements*

Our next remark concerns the set-operations of intersection and union. Remember our initial example? The common part of two lists—the list G of girls and the list L of children who are left-handed—gave us a third list which we denoted by $G \cap L$ and called the intersection of the subsets G and L.

We described this set as follows:

$G \cap L \mathrel{\hat{=}} \{k : k$ is a child who is a girl and who is left-handed$\}$.

Here our description embodies two conditions.
We may also write it as

$G \cap L \mathrel{\hat{=}} \{k : k$ satisfies both the conditions 'This is a child who is a girl' and 'This is a child who is left-handed'$\}$

which, with our symbols for statements, may be written

$G \cap L \mathrel{\hat{=}} \{k : k$ satisfies the statement p_G and $p_L\}$.

The combination 'p and q' occurs so frequently that it is convenient to introduce a notation for it. We write '$p \wedge q$' (read 'p and q'), and regard it as a single statement called the **conjunction** of p and q. Thus we may write

$$G \cap L \mathrel{\hat{=}} \{k : k \text{ satisfies the statement } p_G \wedge p_L\}.$$

Our language offers us a variety of ways of expression for the statement '$p \wedge q$'. For example '$p_G \wedge p_L$' may be written as 'This is a child who is a left-handed girl' or 'This is a child who is left-handed and a girl' or 'This is a child who is both a girl and left-handed' and so on. We are in no doubt that $p_G \wedge p_L$ is the same statement as $p_L \wedge p_G$ (cf. $G \cap L \bumpeq L \cap G$), because it is our language which imposes the restriction on expressing one statement before the other, while our conception of $p_L \wedge p_G$ is of a statement embodying two conditions.

Just as 'and' is the definitive word in forming $A \cap B$ from A and B, so 'and' is the definitive word in forming $p \wedge q$ from p and q.

Exercise 2. Construct single statements, each describing one of the subsets $G \cap L$, $C \cap B$, $G \cap (L \cap V)$, of U.

Exercise 3. For a statement p with corresponding set P, what is the set corresponding to each of the following statements:

$\sim p$, $\sim(\sim p)$, $p \wedge (\sim p)$, $p \wedge p$, $(\sim p) \wedge (\sim p)$, $(\sim p) \wedge p \wedge (\sim p)$, $\sim(p \wedge \sim p)$?

Exercise 4. If p, q correspond to P, Q respectively, what statements correspond respectively to $P \cap Q$, $\tilde{P} \cap Q$, $\tilde{P} \cap \tilde{Q}$, $P \cap \tilde{Q}$, $Q \cap \tilde{Q}$?

Corresponding to the union $G \cup L$ of the sets G and L, we form the single statement 'p_G or p_L', which means 'either p_G, or p_L, or both p_G and p_L'. We denote it by $p_G \vee p_L$ (read p_G or p_L), and call it the **disjunction** of the statements p_L and p_G. Thus

$$G \cup L \bumpeq \{k : k \text{ satisfies the statement } p_L \vee p_G\}.$$

As before, we see that $p_L \vee p_G$ and $p_G \vee p_L$ are one and the same statement (cf. the subset relation $G \cup L \bumpeq L \cup G$). Again, there are many ways of writing the disjunction $p_L \vee p_G$. For example, 'This child either is a girl or is left-handed'; 'This child is a girl or is left-handed'; 'Either this child is a girl, or this child is left-handed, or this child is a left-handed girl' (i.e., sometimes 'either . . . or . . . or both' is used, sometimes 'either . . . or', and sometimes simply 'or'); each means '$p_L \vee p_G$'. 'Or' is never used by us in the exclusive sense of 'or, but not both'; indeed, it is rarely (if ever) used in this way in a mathematical or a logical context.

Exercise 5. Find a single statement for each of the following subsets: $C \cup L$, $S \cup R$, $C \cup S \cup G$. What statement corresponds to $C \cup V$?

Exercise 6. If p corresponds to P, find the set corresponding to each of the following statements: $p \vee p$, $p \vee (\sim p)$, $\sim(p \vee p)$, $\sim(p \vee (\sim p))$.

Exercise 7. If p, q correspond to P, Q respectively, which statements correspond respectively to $P \cup Q$, $\tilde{P} \cup Q$, $P \cup \tilde{Q}$, $\tilde{P} \cup \tilde{Q}$, $P \cup \tilde{P}$?

Exercise 8. Verify that $p \vee (q \vee r) \overset{\frown}{=} (p \vee q) \vee r$.

Exercise 9. Construct English expressions for each of the statements $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$. Are they the same statement?

3.4 *Interpretation of the relation* $\subseteq$

So far, we have been discussing ways of forming statements from simpler statements, based on our methods of forming subsets from essentially simpler subsets. We have in fact developed the analogy between the structure of the subsets of a set and the structure of statements applicable to the elements of that set. Operations such as the union operation (which can be carried out on any two subsets of U) produce analogous operations which combine any two statements applicable to U. A relation between subsets of U does not however produce a new subset, and does not always exist between two arbitrarily chosen subsets of U. Therefore, if it can be stated of two subsets A, B of U that 'A is contained in B', we can reasonably infer the existence of a relationship between the statements corresponding to the subsets A and B respectively—a relationship that will not always exist between two arbitrarily chosen statements applicable to the set U. We explore this idea by returning to our basic example.

Let, as before, $G \overset{\frown}{=} \{k : k \text{ satisfies the statement } p_G\}$
while $V \overset{\frown}{=} \{k : k \text{ satisfies the statement } p_V\}$

where p_V is the statement 'This is a child whose name begins with a vowel'.

We have discovered before that $V \subset G$. In terms of the elements of V, we may express this as follows:

'If we are told that k is an element of V, then we know that k is an element of G'.

Recalling our descriptive definition of the sets V, G, we may now write this as

'If k satisfies the statement p_V, then k satisfies the statement p_G'.

We have here an interpretation, in terms of statements, of the inclusion relation for subsets. Generally, for two subsets P, Q of a set U corresponding to two statements p, q by

$$P \doteq \{k : k \in U, k \text{ satisfies } p\},$$

and

$$Q \doteq \{k : k \in U, k \text{ satisfies } q\},$$

respectively, the subset relation $P \subseteq Q$ can be interpreted as the statement relation

'If $k \in U$ and k satisfies p, then k satisfies q'. There are many ways of expressing this relation: for example

'Whenever k satisfies p, then k also satisfies q', or 'If k satisfies the statement p, then that is sufficient to ensure that k also satisfies the statement q', or 'A sufficient condition for k to satisfy the statement q is that k satisfy the statement p', or 'The statement q is satisfied by k if the statement p is satisfied by k', or 'q is true whenever p is true'.

All of these sentences thus convey the same idea—that the truth of one statement (p) when applied to certain elements guarantees the truth of another statement (q) when applied to those elements. We shall adopt one of the above expressions for this idea, namely

'The truth of the statement p is sufficient for the truth of the statement q', which we shall sometimes abbreviate to

'p is sufficient for q',

and our symbolic notation for the phrase 'is sufficient for' will be $\Rightarrow$. Thus

'$p \Rightarrow q$'

shall be read 'p is sufficient for q'.

All statements, in words or symbols, of the relation '$p \Rightarrow q$' are known as sufficiency conditions for q in terms of p. They assert that if one statement is known to be true, then another statement is also true.

3.5 *Necessity conditions*

We used the subset relation $P \subseteq Q$ to obtain a condition for the truth of the statement q in terms of the truth of the statement p. Now we ask a different question, namely: 'Can we use $P \subseteq Q$ to give us information on the possibility of p being true, supposing we know something of q?'

We answer this question in the following way. $P \subseteq Q$ is the same relation on subsets P, Q as the relation $\tilde{\mathrm{Q}} \subseteq \tilde{\mathrm{P}}$. Now $\tilde{\mathrm{Q}}$ is the subset corresponding to the statement $\sim q$:

$$\tilde{\mathrm{Q}} \bumpeq \{k : k \in \mathrm{U} \text{ and } k \text{ satisfies } \sim q\}.$$

Similarly,

$$\tilde{\mathrm{P}} \bumpeq \{k : k \in \mathrm{U} \text{ and } k \text{ satisfies } \sim p\}.$$

Therefore, by §3.4, $\tilde{\mathrm{Q}} \subseteq \tilde{\mathrm{P}}$ has the following interpretation:

'If we know k satisfies $\sim q$, then we know also that k satisfies $\sim p$'. But this is more simply written as

'If k does not satisfy q, then it cannot satisfy p'.

Therefore, we conclude that the relation $\mathrm{P} \subseteq \mathrm{Q}$ gives us the following condition on p:

'p cannot possibly be satisfied by any k which does not satisfy q'.

This is expressible in a variety of ways, e.g.,

'It is necessary that k satisfy the statement q in order that k satisfy the statement p'.

'The statement p is satisfied by k only if the statement q is satisfied by k'.

'p is false whenever q is false'.

All of these sentences thus convey the same idea, that the falsity of one statement (q) when applied to certain elements guarantees the falsity of another statement (p) when applied to those elements. We shall adopt the following expression as conveyor of this idea:

'The truth of the statement q is necessary for the truth of the statement p',

and we abbreviate this to

'q is necessary for p'.

A separate symbolic notation for the phrase 'is necessary for' could be introduced, but there is no need. For the one subset relation, $\mathrm{P} \subseteq \mathrm{Q}$ leads to both sufficiency and necessity conditions, viz.

'p is sufficient for q'

'q is necessary for p',

so the symbol '$p \Rightarrow q$' already introduced to denote 'p is sufficient for q', also denotes 'q is necessary for p'. The two types of conditions correspond simply to a change of interest: in the one, we are interested in q, and use p; in the other, we are interested in p, and use q. Because of the two types of conditions, the symbol $\Rightarrow$ is often referred to as meaning 'implies'. Thus

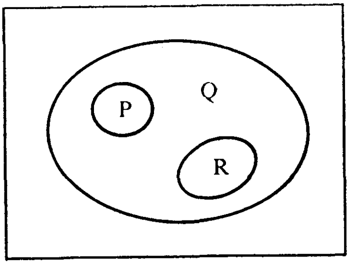
‘$p \Rightarrow q$’

is read ‘p implies q’, and from this it is put into a sufficiency form or a necessity form as desired. Unfortunately, logicians use the word ‘implies’ in a wider sense (see §3.8) so one must exercise care. In this book, except in §3.8, ‘implies’ will always mean the symbol $\Rightarrow$ and thus corresponds to the set relation $\subseteq$.

In passing (since $P \subseteq Q$ is the same relation as $\tilde{Q} \subseteq \tilde{P}$) we have shown that ‘$p \Rightarrow q$’ is the same relation as ‘$\sim q \Rightarrow \sim p$’. We shall recall this point later when discussing methods of proof.

3.6 *Necessary and sufficient conditions*

Consider the diagram:



where we have subsets P, Q, R satisfying $P \subset Q$, $R \subset Q$, $P \cap R = \emptyset$. Suppose these subsets correspond respectively to statements p, q, r, in the usual way. Then the above relations yield

‘$p \Rightarrow q$’,
‘$r \Rightarrow q$’,

and

‘There are no elements which satisfy p and r simultaneously’.

We now infer several important remarks on the interpretation of necessary conditions and sufficient conditions.

(a) p may not be the only statement which implies the statement q. Thus, if p is sufficient for q, there may well be other statements r which are sufficient for q. In fact, r may even be a statement which is true only for elements for which p is false. Hence if $p \Rightarrow q$, it is not necessary for p to be true in order that q be true. Or, simply, if $P \subseteq Q$, p is not in general necessary for q.

(b) (To paraphrase the first sentence of (a)), q may be implied by completely different statements. Thus if q is necessary for p, it may also be necessary for r, where p and r may never be simultaneously satisfied. Hence, if $p \Rightarrow q$, the truth of q is not sufficient to guarantee the truth of p, or simply, if $\mathrm{P} \subseteq \mathrm{Q}$, q is not in general sufficient for p. (a) and (b) both say the same thing, that '$p \Rightarrow q$' and '$q \Rightarrow p$' are not usually the same relation. This is not surprising, for the former corresponds to $\mathrm{P} \subseteq \mathrm{Q}$, and the latter to $\mathrm{Q} \subseteq \mathrm{P}$, and both these relations are not usually simultaneously true.

'$q \Rightarrow p$' is called the converse of '$p \Rightarrow q$', and we have just shown that a relation and its converse are in general distinct relations. Therefore, if one of the relations has been established as valid (e.g., '$p \Rightarrow q$' valid by showing $\mathrm{P} \subseteq \mathrm{Q}$) we are not entitled to assume the validity of the other, but must make a separate investigation. The understanding of this point should help one to detect careless, fallacious arguments (not only on mathematical subjects) in which a result is used to demonstrate a premise, when the opposite is required.

When, then, do '$p \Rightarrow q$' and '$q \Rightarrow p$', yield the same relation? Obviously, since then $\mathrm{P} \subseteq \mathrm{Q}$ and $\mathrm{Q} \subseteq \mathrm{P}$, we have $\mathrm{P} \triangleq \mathrm{Q}$, and so as far as the set U is concerned, p and q are different formulations of the same statement, since each determines the same subset of U.

From '$p \Rightarrow q$' we obtain

'p is sufficient for q' and 'q is necessary for p', while from '$q \Rightarrow p$' we have

'p is necessary for q' and 'q is sufficient for p'.

If both our initial relations are valid, we regroup the above pairs as follows:

'p is sufficient for q and p is necessary for q',

and

'q is sufficient for p and q is necessary for p'.

One of these expressions (say the second) is redundant, as may readily be verified, so we look at the first one. We abbreviate it to 'p is necessary and sufficient for q'.

Various formulations are to be found, e.g.,

'p if and only if q'

'p is sufficient for q and q is sufficient for p'

'p is necessary for q and q is necessary for p', etc.

All such expressions are termed necessary and sufficient conditions, and the two symbols $p \Rightarrow q$ and $q \Rightarrow p$ are in this case condensed into the one: '$p \Leftrightarrow q$' read 'p is equivalent to q'. It is not customary to say 'p is the same as q' as a result of verifying both of the relations '$p \Rightarrow q$' and '$q \Rightarrow p$', because it is assumed that the actual forms of the statements p and q are so different that one could not deduce their identity on U without reasoned argument. For example, it is an early result in deductive plane geometry that the following two dissimilar statements about triangles:

'This triangle has precisely two equal sides' and

'This triangle has precisely two equal angles'

in fact are the same statement: the set of triangles satisfying the former is precisely the set satisfying the latter. So we say the two statements are equivalent, meaning that although we know now that they are one and the same when applied to plane triangles we didn't know initially (although we might have suspected it).

It is rather unfortunate that most of the early theorems one meets in elementary mathematics are statements of necessary and sufficient conditions, i.e., of equivalent statements on a set U. Often, the mathematical examples given either of sufficient or of necessary conditions are ones where the logical point of difference does not appear, paradoxically because the examples are so obvious! For instance, consider

'If a positive integer is divisible by 12, then it is divisible by 3'.

This is true, certainly. The converse,

'If a positive integer is divisible by 3, then it is divisible by 12'

is manifestly false.

Similarly, we would agree that unless a number were divisible by 3, it could not possibly be divisible by 12 (a necessity condition).

In more advanced mathematics, demonstrating the equivalence of (apparently) different statements when applied to a particular set U is often a significant advance and effects much simplification, so its achievement is a comparative rarity in a forest of necessity conditions and sufficiency conditions.

3.7 *Direct and indirect methods of proof*

A 'proof', as in a proof of a theorem, consists of supplying the necessary amount of correct reasoning demonstrating that the truth of one statement (often called the aim or conclusion, say c) is a consequence of the truth of another statement (often called the data or hypothesis, say h). Usually, one is only interested in the cases where the hypothesis h is true initially, so a 'proof' consists of the following: We have a certain set U of elements k; we let

$$H \doteq \{k : k \in U, k \text{ satisfies } h\}$$
$$C \doteq \{k : k \in U, k \text{ satisfies } c\},$$

and we must show $H \subseteq C$; i.e., we must show that the relation '$h \Rightarrow c$' is correct. For example, if

$U \doteq$ the set of proper triangles $\triangle$,

h is the statement '$\triangle$ has exactly two sides equal'

and

c is the statement '$\triangle$ has exactly two angles equal',

so that

$H \doteq$ {triangles with exactly two sides equal}

and

$C \doteq$ {triangles with exactly two angles equal},

then showing either that $H \subseteq C$ or that $h \Rightarrow c$ are each ways of stating the theorem: 'If a triangle has exactly two sides equal, then it has exactly two angles equal'.

In terms of statements, a 'proof' will be a demonstration that '$h \Rightarrow c$' is a correct relation between the statements h and c.

There are two ways of obtaining such a proof.

(a) A direct method of proof. The hypothesis h is used as starting point, and by one or more steps of reasoning, the conclusion is obtained. This corresponds to verifying $h \Rightarrow c$.

(b) An indirect method of proof. The conclusion c is assumed to be false, and the statement $\sim c$ is used as starting point. Then, by one or more steps of reasoning, the statement $\sim h$ is attained. This corresponds to verifying $\sim c \Rightarrow \sim h$.

In (a), the argument is completed as follows: '$h \Rightarrow c$' means that c is true whenever h is true. For the elements we are considering, h is true. Therefore c is true.

In (b), the argument is completed as follows:

either '$\sim c \Rightarrow \sim h$' and '$h \Rightarrow c$' are known to be equivalent relations, therefore we may replace '$\sim c \Rightarrow \sim h$' by '$h \Rightarrow c$' and complete the argument as for (a),

or '$\sim c \Rightarrow \sim h$' means that if c is assumed to be false, then h is also false. But, for the elements we are considering, h is known to be true. Since h cannot be both true and false for the same elements, we have a contradiction. This contradiction can only be resolved by admitting that an incorrect assumption has been made, i.e., c is not false, but true. Thus, whenever h is true, c is true.

Example: We wish to show that whenever a triangle has exactly two sides equal (h), it has exactly two angles equal (c).

Direct method: We suppose h is true, and so we start with a triangle say ABC, in which AB, AC have equal lengths, each unequal to the length of BC, and deduce (using, say, certain axioms on the congruence of triangles) that the angles ABC, ACB are equal in magnitude and unequal to the magnitude of the angle BAC.

Indirect method: We suppose $\sim c$ is true, so we start with a triangle in which either all three angles are equal (one case) or no two angles are equal (a second case) and show that either case leads to the result $\sim h$. (In the first case we show all the sides are equal; in the second we show no two sides are equal.)
Then, since we are concerned only with those triangles for which h is true, we must have also that c is true (since whenever c is false we have triangles which do not satisfy h).

A fallacious proof of '$h \Rightarrow c$' will usually suffer from one or more of the following errors:

(i) The reasoning used to demonstrate $h \Rightarrow c$ (or $\sim c \Rightarrow \sim h$) is either incorrect, or perhaps is valid in certain special cases only—cases too specialised to cover all possibilities allowed by the hypothesis h.

(ii) Instead of proving $h \Rightarrow c$, the reasoning shows that $c \Rightarrow h$, i.e., conclusion and hypothesis have been interchanged. Since $h \Rightarrow c$ and $c \Rightarrow h$ are in general different relations, there is no 'proof' at all.

(iii) Instead of proving $h \Rightarrow c$, the reasoning shows that $\sim h \Rightarrow \sim c$, i.e., what has been 'proved' is the relation 'c is false whenever h is false'. This is equivalent to the relation 'h is true whenever c is true', i.e. to $c \Rightarrow h$, and so again the 'proof' is invalid.

Exercise 10. Let U $\doteq$ the set of counting numbers.

h is the statement 'k is a prime number greater than 2'.
c is the statement 'k is an odd number'.

Prove $h \Rightarrow c$ using both direct and indirect arguments. Show that $c \Rightarrow h$, $\sim h \Rightarrow \sim c$ are each incorrect relations.

3.8 *The logician's term 'implies'*

In §3.4, we developed the relation $p \Rightarrow q$ between statements by analogy with the relation $P \subseteq Q$ between subsets, where

$$\mathrm{P} \doteqdot \{k : k \text{ satisfies } p\},$$

and

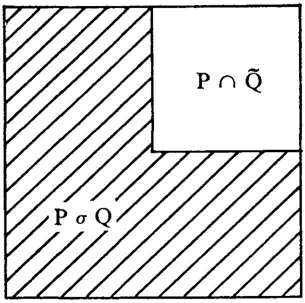
$$\mathrm{Q} \doteqdot \{k : k \text{ satisfies } q\}.$$

Logicians prefer to be rather more careful, as we shall now explain. From any two statements p and q, they construct a new statement, $p \rightarrow q$ (read 'p implies q' or 'the conditional statement with antecedent p and consequent q') by the rule that $p \rightarrow q$ is the statement corresponding to the subset P σ Q introduced earlier (see §2.7). Thus

$$\mathrm{P}\,\sigma\,\mathrm{Q} \doteqdot \{k : k \text{ satisfies } p \rightarrow q\}.$$

We see therefore that 'implies' here, denoted by →, is the operation on statements p, q which corresponds to the σ operation on subsets P, Q.

Recalling that $\mathrm{P}\,\sigma\,\mathrm{Q} \doteqdot \tilde{\mathrm{P}} \cup \mathrm{Q}$, with diagram:


$\mathrm{P} \cap \tilde{\mathrm{Q}}$
$\mathrm{P}\,\sigma\,\mathrm{Q}$

we have the alternative formulation:

'$p \rightarrow q$' is that statement formed from p and q which is satisfied by all elements of U except those which satisfy p but do not satisfy q.

The previous discussion on sufficiency and necessity conditions throws light on the following reason for calling $p \rightarrow q$ 'p implies q': by the word 'implies', as used in ordinary speech, we intend to convey the idea that the truth of one statement (say q) is a consequence of the truth of another (say p). But p may be false. When this is the case we do not exclude the possibility that q may be true, nor do we exclude the possibility that q may be false if p is false. We do emphatically deny that one possibility may occur; that q is false while p is true. Therefore, the statement 'p implies q' can really only be regarded as being false when this last case arises (p true and q false). So in all other cases, we shall regard 'p implies q' as being a true statement. Thus the subset of elements of U for which 'p implies q' is satisfied is the complement of the subset

$$\{k : k \in \mathrm{U},\ k \text{ satisfies } p \text{ but does not satisfy } q\}$$

$$\bumpeq \{k : k \in \mathrm{P} \text{ and } k \in \tilde{\mathrm{Q}}\}$$
$$\bumpeq \{k : k \in \mathrm{P} \cap \tilde{\mathrm{Q}}\}.$$

So, the subset corresponding to $p \rightarrow q$ is $\widetilde{(\mathrm{P} \cap \tilde{\mathrm{Q}})} \bumpeq \tilde{\mathrm{P}} \cup \mathrm{Q} \bumpeq \mathrm{P}\, \sigma\, \mathrm{Q}$.

For example, returning to $\mathrm{U} \bumpeq$ {children in the class}, '$p_L \rightarrow p_G$' is the statement corresponding to the subset

$\tilde{\mathrm{L}} \cup \mathrm{G} \bumpeq$ {children who are right-handed or who are girls}

$$\bumpeq \{C, D, E, G, H, I, K, N, O, P, Q, R, S, T, U, W, Y, A, L, M, V\}$$

On examining this list of names, it will be observed that we have included both girls and boys, right-handers and left-handers, but the only left-handers appearing are girls. In other words, if a child in $\mathrm{L}\, \sigma\, \mathrm{G}$ is left-handed, then that child is a girl. $\mathrm{L}\, \sigma\, \mathrm{G}$ contains other children, but no other left-handed children. Thus the possibility of left-handed boys appearing in $\mathrm{L}\, \sigma\, \mathrm{G}$ is excluded, but right-handed children, both girls and boys, do belong to $\mathrm{L}\, \sigma\, \mathrm{G}$. This is precisely the significance of the logician's statement '$p_L \rightarrow p_G$'. It determines a subset in which if an element satisfies p_L, then that element also satisfies p_G. Nothing is said regarding any of its elements which do not satisfy p_L.

Exercise 11. Prove that $\mathrm{P}\, \sigma\, \mathrm{Q} \bumpeq (\mathrm{P} \cap \mathrm{Q}) \cup \tilde{\mathrm{P}}$ and deduce that $p \rightarrow q$ and $(p \wedge q) \vee ({\sim}p)$ are equivalent statements.

Exercise 12. Prove that $\mathrm{P}\, \sigma\, \mathrm{Q} \bumpeq \tilde{\mathrm{Q}}\, \sigma\, \tilde{\mathrm{P}}$, and deduce that $p \rightarrow q$ and ${\sim}q \rightarrow {\sim}p$ are equivalent statements. How would you write the implication ${\sim}p_G \rightarrow {\sim}p_L$ in words? ($p_L \rightarrow p_G$ gave 'If the child is left-handed, then the child is a girl'.)

Exercise 13. Prove that $(p \wedge (p \rightarrow q)) \Rightarrow q$. This should provide further clarification of $\rightarrow$ and $\Rightarrow$.

Exercise 14. What subset of U corresponds to the statement $(p \wedge (p \rightarrow q)) \rightarrow q$?

Exercise 15. (i) Prove that $(\mathrm{P} \cap \mathrm{Q})\, \sigma\, \mathrm{R} \bumpeq (\mathrm{P} \cap \tilde{\mathrm{R}})\, \sigma\, \tilde{\mathrm{Q}}$.

(ii) Find two statements of the form $(x \wedge y) \rightarrow z$, where (x, y, z) is some arrangement of (p or ${\sim}p$, q or ${\sim}q$, r or ${\sim}r$) which are equivalent to $(p \wedge q) \rightarrow r$.

(iii) Write out these three statements when p is '$\mathrm{X} > 0$', q is '$\mathrm{X} < \frac{1}{2}$', r is '$\mathrm{X}^2 < \mathrm{X}$'.

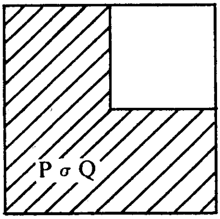
From the statements $p \rightarrow q$ and $q \rightarrow p$ the conjunction

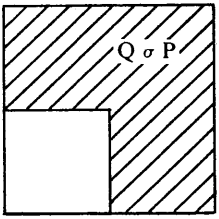
$$(p \rightarrow q) \wedge (q \rightarrow p)$$

may be formed; it corresponds to the subset

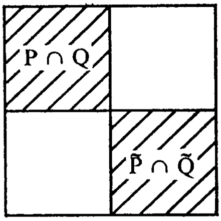
$$\begin{aligned}(\mathrm{P}\ \sigma\ \mathrm{Q}) \cap (\mathrm{Q}\ \sigma\ \mathrm{P}) &\bumpeq (\tilde{\mathrm{P}} \cup \mathrm{Q}) \cap (\tilde{\mathrm{Q}} \cup \mathrm{P}) \\ &\bumpeq ((\tilde{\mathrm{P}} \cup \mathrm{Q}) \cap \tilde{\mathrm{Q}}) \cup ((\tilde{\mathrm{P}} \cup \mathrm{Q}) \cap \mathrm{P}) \\ &\bumpeq ((\tilde{\mathrm{P}} \cap \tilde{\mathrm{Q}}) \cup (\mathrm{Q} \cap \tilde{\mathrm{Q}})) \cup ((\tilde{\mathrm{P}} \cap \mathrm{P}) \cup (\mathrm{Q} \cap \mathrm{P})) \\ &\bumpeq (\mathrm{P} \cap \mathrm{Q}) \cup (\tilde{\mathrm{P}} \cap \tilde{\mathrm{Q}}),\end{aligned}$$

which is easily seen by the diagrams:





(P σ Q) ∩ (Q σ P)



Thus $(p \rightarrow q) \wedge (q \rightarrow p)$ is the statement corresponding to the subset $(\mathrm{P} \cap \mathrm{Q}) \cup (\tilde{\mathrm{P}} \cap \tilde{\mathrm{Q}})$. It is usually called the biconditional statement formed from p and q, and denoted by $p \leftrightarrow q$. Clearly $p \leftrightarrow q$ and $q \leftrightarrow p$ are the same statement. Its properties are explored in the following exercises.

Exercise 16. What is the subset corresponding to the statement $p \leftrightarrow p$?

Exercise 17. What subset corresponds to the statement $p \wedge (p \leftrightarrow q)$? Verify that $(p \wedge (p \leftrightarrow q)) \Rightarrow q$.

Exercise 18. Verify similarly that $(q \wedge (p \leftrightarrow q)) \Rightarrow p$.

Exercise 19. Show that $(p \wedge (p \leftrightarrow q)) \Leftrightarrow (q \wedge (p \leftrightarrow q))$.

3.9 *Summary*

A 'statement' is a statement about the elements of a set U which, when applied to an element of U, gives either a correct or an incorrect description of that element, but never both descriptions simultaneously.

By the simple process of relating a statement p to a subset P of U by the correspondence

$$\mathrm{P} \bumpeq \{k : k \in \mathrm{U} \text{ and } k \text{ satisfies } p\},$$

we have built up a 'statement-algebra' from the set-algebra, which, in effect, has led us to analyse the way in which statements are converted (by the use of words such as 'not', 'and', 'or') into different statements. We formed the negation $\sim p$ (corresponding to $\tilde{\mathrm{P}}$), the conjunction $p \wedge q$ (corresponding to $\mathrm{P} \cap \mathrm{Q}$), and the disjunction $p \vee q$ (corresponding to $\mathrm{P} \cup \mathrm{Q}$).

The existence of a subset relation $\mathrm{P} \subseteq \mathrm{Q}$ led to the existence of a corresponding relation (which we called 'p implies q' and denoted by $p \Rightarrow q$), usually expressed in the form 'If we know an element satisfies p, then it also satisfies q'. Examination of this relation from two points of view then led to the following classifications:

(a) Conditions which use $p \Rightarrow q$ to assert the truth of q are known as sufficiency conditions for q in terms of p;

(b) conditions which use $p \Rightarrow q$ to cast doubt on the truth of p are known as necessity conditions for p in terms of q; and some of the variety of expressions of such conditions were listed in each case.

The equivalence of the subset relations $\mathrm{P} \subseteq \mathrm{Q}$, $\tilde{\mathrm{Q}} \subseteq \tilde{\mathrm{P}}$ led to identification of the relations $p \Rightarrow q$ and $\sim q \Rightarrow \sim p$. Thus

'If we know k satisfies p, then k satisfies q' and

'If we know k does not satisfy q, then k does not satisfy p'

are two expressions for the same relation between p and q.

However, we showed by a simple example that $p \Rightarrow q$ and the converse relation $q \Rightarrow p$ express two distinct relations between p and q; further, it is generally the case that if one relation holds, the other does not. Hence, establishing the relation

'If we know k satisfies q, then k satisfies p'

has no connection with (and is not a proof of) the validity of the relation

'If we know k satisfies p, then k satisfies q'.

In the exceptional case where both relations $p \Rightarrow q$, $q \Rightarrow p$ hold between p and q, we say p and q are equivalent statements on the set U, and write $p \Leftrightarrow q$. A common expression for the equivalence of p and q is

'A necessary and sufficient condition that k satisfy q is that we know k satisfies p', or

'k satisfies q if and only if we know k satisfies p'.

Finally, the conditional statement or implication $p \rightarrow q$ used by logicians was introduced as the statement corresponding to the subset $\mathrm{P}\,\sigma\,\mathrm{Q} \bumpeq \tilde{\mathrm{P}} \cup \mathrm{Q}$. Whereas, in relations such as $p \Rightarrow q$, one deals only with those elements k for which p is satisfied, $p \rightarrow q$

treats all elements k of U on an equal footing. It is usually expressed as

'If k satisfies p, then k satisfies q' (i.e., it is no longer supposed that we know k satisfies p). $p \rightarrow q$ is related to $p \Rightarrow q$ by the relation $(p \wedge (p \rightarrow q)) \Rightarrow q$.

Chapter 4

BOOLEAN ALGEBRA

4.1 *A change of viewpoint*

The ideas introduced in Chapter 1, the operations introduced in Chapter 2, and indeed the whole line of development so far has hinged on one basic notion—that sets and subsets are identified by their constituent elements. However, we have gradually become more interested in the relations existing among the subsets of a set, and have paid less attention to the actual composition of (i.e., to the elements composing) a given subset.

In other words, our attention is being increasingly directed to a study of the interplay between subset operations and subset relations. The methods used are based on the properties possessed by these operations and relations rather than on the reduction of all subsets to their constituent elements. For example, to show that for any three subsets X, Y, Z of U, $(X \mathbin{\sigma} Y) \mathbin{\sigma} Z \subseteq X \mathbin{\sigma} (Y \mathbin{\sigma} Z)$, we proceed as follows:

$$
\begin{aligned}
(X \mathbin{\sigma} Y) \mathbin{\sigma} Z &\bumpeq (\tilde{X} \cup Y) \mathbin{\sigma} Z && \text{(definition of } \sigma\text{)}\\
&\bumpeq \widetilde{(\tilde{X} \cup Y)} \cup Z && \text{(definition of } \sigma\text{)}\\
&\bumpeq (\tilde{\tilde{X}} \cap \tilde{Y}) \cup Z && \text{(property of } \sim\text{)}\\
&\bumpeq (X \cap \tilde{Y}) \cup Z. && \text{(property of } \sim\text{)}\\
X \mathbin{\sigma} (Y \mathbin{\sigma} Z) &\bumpeq X \mathbin{\sigma} (\tilde{Y} \cup Z) && \text{(definition of } \sigma\text{)}\\
&\bumpeq \tilde{X} \cup (\tilde{Y} \cup Z) && \text{(definition of } \sigma\text{)}\\
&\bumpeq (\tilde{X} \cup \tilde{Y}) \cup Z. && \text{(property of } \cup\text{)}
\end{aligned}
$$

But $\quad X \cap \tilde{Y} \subseteq \tilde{Y},\qquad$ (property of $\cap$)

while $\quad \tilde{X} \cup \tilde{Y} \supseteq \tilde{Y},\qquad$ (property of $\cup$)

hence $\quad X \cap \tilde{Y} \subseteq \tilde{X} \cup \tilde{Y}.\qquad$ (property of $\subseteq$)

Hence finally

$$(X \cap \tilde{Y}) \cup Z \subseteq (\tilde{X} \cup \tilde{Y}) \cup Z \qquad \text{(property of } \cup\text{)}$$

and so

$$(X \mathbin{\sigma} Y) \mathbin{\sigma} Z \subseteq X \mathbin{\sigma} (Y \mathbin{\sigma} Z).$$

Here, our argument has used certain of the properties possessed by the operations $\cup$, $\cap$, $\sim$ and the relation $\subseteq$. Less obviously, we have also used some of the properties of the relation $\bumpeq$. Of course, all of these properties were initially established by examining the definitions of the various relations and operations—definitions which were given explicitly in terms of the elements of the subsets occurring.

We therefore have the following situation: the operations and relations introduced have been defined in terms of the elements of subsets. From these definitions many properties have been derived—properties which enable us to replace one symbol for a subset by another symbol which is more useful in a given problem. [For example,

$$\tilde{X} \cup (\tilde{Y} \cup Z) \bumpeq (\tilde{X} \cup \tilde{Y}) \cup Z$$

states that the subset denoted by $\tilde{X} \cup (\tilde{Y} \cup Z)$ is the same set as the subset denoted by $(\tilde{X} \cup \tilde{Y}) \cup Z$. This is a consequence of the associativity of the union operation, which is itself a consequence of the definition of the union operation.] Systematic application of this idea allows us to solve problems in which subsets are denoted by symbols, without introducing elements.

Can we find a way of analysing operations on subsets of a set which does not explicitly involve their elements? Our remarks show that no such way is possible if we use the given definitions of the operations and relations, since each one involves elements. Moreover, subsets have been defined by their constituent elements, so our task seems hopeless. We can partially overcome the difficulties concerned with operations and relations by defining them anew, and specifying in their new definitions all the properties of the operations that had been derived directly from their previous definitions.

So conceivably we can introduce 'new' relations denoted by $\bumpeq$ and $\subseteq$, and 'new' operations denoted by $\cup$, $\cap$ and $\sim$, each of which will possess by definition the appropriate properties for it to be a direct copy, or model, of the originally introduced relation or operation denoted by the same symbol.

Subsets present a more difficult problem, which we attack as follows. Although a subset is defined by its elements, we are here really interested in the different symbols which may be used to denote it.

Suppose for example that in a given set U subsets A, B, C, D have been specified. Form all possible meaningful combinations of A, B, C, D with the operations $\cap$, $\cup$, $\sim$. Then we are interested more with the existence of either of the relations $\subset$ or $\bumpeq$ between pairs of such combinations than we are with the composition of the resulting subsets. Therefore, let us regard A, B, C, D, etc., not as symbols denoting subsets of U, but simply as objects on which the operations will act in accordance with specified rules. Before we pursue this idea, we must investigate an immediate side effect produced by the changed role of A, B, C, . . . Formerly, the relation $A \bumpeq C$ was a statement of the fact that A and C denoted the same subset, viz. 'The subset denoted by A is the same set as the subset denoted by C.'

In terms avoiding the use of 'subset', this relation may be stated: 'Whenever A appears in any symbol we may replace it, if we so desire, by C, and vice versa, without altering the meaning of that symbol' (e.g., if $A \bumpeq C$ then each of $(A \cap B) \cup C$, $(A \cap B) \cup A$, $(C \cap B) \cup A$ denotes the same subset). Regarding A and C as objects, we see that the natural interpretation of $A \bumpeq C$ is now 'A **can be replaced by** C'. To emphasise this alteration in meaning we shall denote the phrase 'can be replaced by' by the symbol $\leftrightharpoons$, rather than by $\bumpeq$, but the properties we specify for $\leftrightharpoons$ will be the analogues of those possessed by $\bumpeq$.

With these remarks in mind, let us try to build up the new system. We shall see that the changed role of A, B, C, . . . will require accurate specification of the relations and operations we wish to use.

4.2 *Specifying relations and operations*

We start with objects A, B, C, . . . on which we wish to define certain relations and certain operations. Our aim is to imitate exactly the situation in which A, B, C, . . . are symbols for subsets of a set U.

(i) In laying down the definitions, we shall find it convenient to use symbols such as X, Y, Z as 'placeholders' for the objects A, B, C. Whenever X, Y, Z, ... are replaced by objects chosen from A, B, C, ... (X is replaced by the same object wherever it occurs in the one statement, etc.) we have a statement of a relation existing among the chosen objects.

(ii) The relation 'can be replaced by' is denoted by $\leftrightharpoons$.

We require $\leftrightharpoons$ to have precisely the properties of the phrase (used on sets) 'is the same set as'. Let us tabulate these properties.

(a) $\bumpeq$ is a relation between pairs of subsets (such relations are called 'binary relations').

(b) For all X, $X \bumpeq X$ (reflexive property).

(c) If $X \bumpeq Y$, then also $Y \bumpeq X$ (symmetric property).

(d) If $X \bumpeq Y$, and if $Y \bumpeq Z$, then $X \bumpeq Z$ (transitive property).

You may ask here 'Is it necessary to have specified (explicitly) all four'? The answer is 'yes', because each of (a), (b), (c), (d) expresses an independent property of the phrase 'is the same set as'. Is it necessary to specify these as defining properties? The answer is again 'yes', because we are not using $\leftrightharpoons$ as a symbol derived from the phrase 'is the same set as' in the sense that all the obvious properties of the phrase are vested in the symbol. We are trying to build up a theory which models the symbolism already developed, but which is self-contained. Hence we cannot assume that $\leftrightharpoons$ inherits any properties, because now, none of our symbols has any ancestors (nor even a collective unconscious!). So we have to specify all the properties of $\leftrightharpoons$ that we wish to use, and naturally, we specify the properties that we would like it to have if it is going to behave like 'is the same set as'. Often, the difficulty is one of realising how many properties of a symbol have to be specified before that symbol can be regarded as a 'model' for a concrete operation!

Therefore, we define $\leftrightharpoons$ as follows:

(a) $\leftrightharpoons$ is a relation between pairs of objects.

(b) For all X, $X \leftrightharpoons X$ (reflexive property).

(c) If $X \leftrightharpoons Y$, then also $Y \leftrightharpoons X$ (symmetric property).

(d) If $X \leftrightharpoons Y$ and if $Y \leftrightharpoons Z$, then $X \leftrightharpoons Z$ (transitive property).

(iii) The other relation we must imitate is 'is contained in'. So we introduce a binary relation, which we shall call 'is contained in', and denote by $\subseteq$. We specify the following properties of $\subseteq$:

(a) $X \subseteq X$ (reflexive property).

(b) If $X \subseteq Y$ and if $Y \subseteq Z$, then $X \subseteq Z$ (transitive property).

(c) If $X \subseteq Y$ and if $Y \subseteq X$, then $X \leftrightharpoons Y$.

(iv) We use $\subseteq$ to specify two particular objects of our collection: There is an object $\emptyset$ which has the property that for all X, $\emptyset \subseteq X$.

There is an object U which has the property that for all X, $X \subseteq U$.

We must now define operations corresponding to intersection, union, and complementation by specifying the properties which characterise these operations.

(v) The intersection operation, denoted by $\cap$. $\cap$ is a binary operation, and its action on the pair X, Y will be denoted by $X \cap Y$. Its properties are:

(a) For every X and Y, $X \cap Y$ can be replaced by Z for some object Z (e.g., $A \cap B$ can be replaced by at least one of A, B, C, . . .). This corresponds to the fact that if A, B are subsets of U, so is $A \cap B$. An operation which does not produce 'new' objects when applied to a collection of objects is said to be a closed operation on that collection. For example, + is a closed operation on the counting numbers ($x+y$ is a counting number if x, y are), $\div$ is not a closed operation on the counting numbers (x/y is not always a counting number when x, y are), but $\div$ is a closed operation on the positive rationals (x/y is a positive rational if x, y are).

(b) For every X and Y, $X \cap Y \leftrightharpoons Y \cap X$, i.e., $\cap$ is a commutative operation.

(c) For every X, Y, Z, $X \cap (Y \cap Z) \leftrightharpoons (X \cap Y) \cap Z$, i.e., $\cap$ is an associative operation.

(d) $[X \subseteq Y] \Leftrightarrow [X \cap Y \leftrightharpoons X]$.

(vi) The union operation, denoted by $\cup$. $\cup$ is a binary operation, and its action on the pair X, Y will be denoted by $X \cup Y$. Its properties are:

(a) For every X and Y, there is a Z for which $X \cup Y \leftrightharpoons Z$ (i.e., $\cup$ is a closed operation on A, B, C, . . .).

(b) For every X and Y, $X \cup Y \leftrightharpoons Y \cup X$, i.e. $\cup$ is commutative.

(c) For every X, Y, Z, $X \cup (Y \cup Z) \leftrightharpoons (X \cup Y) \cup Z$, i.e., $\cup$ is associative.

(d) $[X \subseteq Y] \Leftrightarrow [X \cup Y \leftrightharpoons Y]$.

Since $\cap$ and $\cup$ are each closed, commutative, associative binary operations, properties (a), (b), (c) do not distinguish them. Property (d), which connects each operation with the relation $\subseteq$, characterises $\cap$, $\cup$ respectively.

(vii) The complementation operation, denoted by $\sim$. (This is rather hard to specify without using elements.)

$\sim$ is a unary operation (i.e. it acts on a single object) and its action on X will be denoted by $\tilde{X}$. Its properties are:

(a) For every X, $\tilde{X} \leftrightharpoons Z$ for some Z, i.e., $\sim$ is a closed operation.
(b) For every X, $X \cup \tilde{X} \leftrightharpoons U$ and $X \cap \tilde{X} \leftrightharpoons \emptyset$.
(c) For every X, $(\tilde{\tilde{X}}) \leftrightharpoons X$. ($(\tilde{\tilde{X}})$ will mostly be written $\tilde{\tilde{X}}$.)
(d) For every X and Y, $(\widetilde{X \cup Y}) \leftrightharpoons \tilde{X} \cap \tilde{Y}$.
(e) For every X and Y, $(\widetilde{X \cap Y}) \leftrightharpoons \tilde{X} \cup \tilde{Y}$.

It is reasonable to suppose that all of (a) . . . (e) are (at least) necessary to specify the operation $\sim$. We can however easily show that (e) is a consequence of the preceding properties. By (a), we may use $\tilde{X}$, $\tilde{Y}$ in (d) (since they can be replaced by objects of the collection). Hence

$$\widetilde{\tilde{X} \cup \tilde{Y}} \leftrightharpoons \tilde{\tilde{X}} \cap \tilde{\tilde{Y}}.$$

By (c), we have $\widetilde{\tilde{X} \cup \tilde{Y}} \leftrightharpoons X \cap Y$, which on applying $\sim$ and using (c) again, gives

$$\tilde{X} \cup \tilde{Y} \leftrightharpoons \widetilde{X \cap Y},$$

i.e., (e). Later (see §4.3), we shall comment further on this aspect of specifying redundant properties.

We add more properties which must be explicitly specified in our system, namely
(viii) The distributive laws:

$$X \cap (Y \cup Z) \leftrightharpoons (X \cap Y) \cup (X \cap Z),$$
$$X \cup (Y \cap Z) \leftrightharpoons (X \cup Y) \cap (X \cup Z).$$

4.3 *Construction and use of a mathematical model*

Surely no one will dispute the fact that our system—that is the objects A, B, . . . , U, together with the relations denoted by $\leftrightharpoons$ and $\subseteq$, and the operations denoted by $\cap$, $\cup$, and $\sim$ (which have only the properties specified above)—models the account of our theory of sorting processes, with the exception that instead of using symbols to denote words and phrases, we have regarded symbols as the objects of discussion, and used words and phrases to specify the properties of relations and operations which are introduced by definition—they are not physical operations or relations on the objects, but are given solely by their respective defining properties. What we have just done is usually referred to as the formulation of a mathematical model, or as the setting up of an abstract system.

It consists precisely of using a previously encountered problem as a motivation for specifying the initial properties of various symbols. The symbols themselves are regarded as having only the properties specified. By using these properties, and only these properties, one tries to obtain as many new results as possible about the system. How are results obtained? By using the specified properties to deduce further properties. What is meant by 'deduce'? Our answer here is 'obtain by correct reasoning', and we will not be drawn further.

We make three points:

(1) The 'new results' that we try first to obtain in our system will be those results suggested to us by analogy with the results obtained in the initial 'concrete' problem. If we find that after prolonged effort we cannot deduce some such analogous results, there are three possibilities:

(a) we haven't tried hard enough;

(b) our original result may be wrong, so perhaps we should go back and see how we obtained it;

(c) we may have forgotten to specify enough properties when we constructed our abstract system.

Naturally, being loath to accept (a), we try (b). If we can justify the original argument, then we have to resort to (c). We look at the result that we are trying to prove, and try to pick some additional information which, if permitted, would enable us to deduce that result. We then add this information to our initial list of properties (thus regarding it as something inadvertently left out at the beginning). Should (b) and (c) both fail us, we accept (a), and try again.

(2) It may happen that we have been careless in specifying the properties of the system; so much so that we find ourselves deriving contradictory conclusions by correct reasoning. If that happens, we must take a very long look at our initial premises and identify the ones responsible for the contradictions. Then we must decide which of these we do not want, and discard them. We may of course have to introduce some more properties to cover some non-contradictory aspects of the discarded ones that we wish to preserve.

(3) We may discover that some of the properties initially specified may be derived entirely from the remaining ones, i.e., that we have rather more than required for our purposes. Then we are at liberty

to remove the redundancies, and work with the smaller set of specifications. It is often of considerable interest to find the smallest set of premises sufficient to derive a complete model system.

4.4 *An axiom system for Boolean algebra*

Briefly, the desirable features of an abstract system devised on the basis of its imitating a real system are that its specifications (or axioms) are consistent (i.e., do not lead to contradictions) and complete (i.e., are sufficient to produce all results suggested by analogy with the real system). Any system possessing these two features may then be examined for independence, i.e., one tries to replace its axioms by a simpler set, and so on until no further simplification is possible if consistency and completeness are to be preserved.

The real system we have been discussing is called an algebra of subsets of U. 'Algebra' is used here to mean 'a non-empty collection of subsets which, whenever it contains A also contains $\tilde{A}$, and whenever it contains A and B also contains $A \cap B$ and $A \cup B$'. U is always regarded as having some elements, and so Ø and U are two distinct subsets belonging to any such algebra ($Ø \leftrightarrows A \cap \tilde{A}$ and $U \leftrightarrows A \cup \tilde{A}$, so each does belong to the algebra).

The abstract system we wish to formulate is called a Boolean algebra. It consists of (a) a set of objects, A, B, C, . . . which contains two distinct objects Ø and U, and (b) the following operations: a binary operation $\cup$ called union; a binary operation $\cap$ called intersection; and a unary operation $\sim$ called complementation. There is also a relation $\leftrightarrows$ usually called equality but which we shall call replaceability. The following axioms are satisfied.

1. $\leftrightarrows$ is reflexive, symmetric, and transitive; i.e., $A \leftrightarrows A$, if $A \leftrightarrows B$ then $B \leftrightarrows A$, and if $A \leftrightarrows B$ and $B \leftrightarrows C$ then $A \leftrightarrows C$.
2. If $A \leftrightarrows B$, then $A \cap C \leftrightarrows B \cap C$ for all C.
3. If $A \leftrightarrows B$, then $\tilde{A} \leftrightarrows \tilde{B}$.
4. For all A, B, C,

$$A \cup (B \cup C) \leftrightarrows (A \cup B) \cup C,$$
$$A \cap (B \cap C) \leftrightarrows (A \cap B) \cap C.$$

5. For all A, B,

$$A \cup B \leftrightarrows B \cup A,$$
$$A \cap B \leftrightarrows B \cap A.$$

6. For all A, B, C,

$$A \cup (B \cap C) \leftrightharpoons (A \cup B) \cap (A \cup C),$$
$$A \cap (B \cup C) \leftrightharpoons (A \cap B) \cup (A \cap C).$$

7. For all A,

$$A \cup \emptyset \leftrightharpoons A \quad \text{and} \quad A \cap U \leftrightharpoons A.$$

8. For each A,

$$A \cup \tilde{A} \leftrightharpoons U \quad \text{and} \quad A \cap \tilde{A} \leftrightharpoons \emptyset.$$

Axioms 1, 2, 3 say that $\leftrightharpoons$ is a model for the relation 'is the same set as'. Axioms 4, 5, 6 specify $\cup$ and $\cap$. Axiom 7 specifies the particular nature of $\emptyset$ and U, while axiom 8 specifies the complement $\tilde{A}$ of A. We have not yet formally introduced $\subseteq$ but we shall do so later.

Many obvious properties of the real system not explicitly stated in the above axiom system must now be established, so that they may be used. Firstly, we point out the principle of duality for Boolean algebras. The dual statement of a given statement (involving the objects and operations just specified) is obtained by replacing $\cup$ by $\cap$, $\cap$ by $\cup$, $\emptyset$ by U and U by $\emptyset$. We now observe that our axioms contain, with any one axiom, the dual of that axiom. Hence any theorem we obtain yields a 'free' or 'bonus' theorem, namely its dual. To prove the dual theorem, we have only to replace each step in the original proof by its dual. This is the principle of duality for the present theory.

First 'obvious' result: U is unique (analogue of the unique initial set U), i.e., if W satisfies the defining properties of U, then U $\leftrightharpoons$ W.

Proof: Suppose another object W has the characteristic property of U. By axiom 7, this means for all A,

$$A \cap W \leftrightharpoons A \quad \text{as well as} \quad A \cap U \leftrightharpoons A.$$

Put A $\leftrightharpoons$ U in the first, A $\leftrightharpoons$ W in the second. Then

$$U \cap W \leftrightharpoons U \quad \text{and} \quad W \cap U \leftrightharpoons W.$$

But, by axiom 5, $U \cap W \leftrightharpoons W \cap U$. Hence

$$U \leftrightharpoons W.$$

Corollary: By the principle of duality, $\emptyset$ is unique.

Second 'obvious' result: Each element A has a unique complement $\tilde{A}$.

Proof: Suppose another object, say A′, has the characteristic properties of $\tilde{A}$; i.e. by axiom 8,

$$A \cup A' \leftrightharpoons U \quad \text{and} \quad A \cap A' \leftrightharpoons \varnothing.$$

Now by axiom 7, applied to $\tilde{A} \cap A'$, we have

$$\tilde{A} \cap A' \leftrightharpoons (\tilde{A} \cap A') \cup \varnothing.$$

Writing $\varnothing \leftrightharpoons \tilde{A} \cap A$, and using the distributive law, we have

$$\tilde{A} \cap A' \leftrightharpoons (\tilde{A} \cap A') \cup (\tilde{A} \cap A) \leftrightharpoons \tilde{A} \cap (A' \cup A) \leftrightharpoons \tilde{A} \cap U \leftrightharpoons \tilde{A},$$

while a similar argument with $\varnothing \leftrightharpoons A' \cap A$ gives

$$\tilde{A} \cap A' \leftrightharpoons A'.$$

Hence $A' \leftrightharpoons \tilde{A}$, i.e. complement is unique.

Exercise 1. Using only the axioms given, prove each of the following 'obvious results':

(i) $(\tilde{\tilde{A}}) \leftrightharpoons A$ for all A.

(ii) $A \cup U \leftrightharpoons U$ and $A \cap \varnothing \leftrightharpoons \varnothing$ for all A.

(iii) $A \cup A \leftrightharpoons A \cap A \leftrightharpoons A$ for all A.

(iv) $A \cup (A \cap B) \leftrightharpoons A$ and $A \cap (A \cup B) \leftrightharpoons A$ for all A and B.

(v) $\widetilde{(A \cup B)} \leftrightharpoons \tilde{A} \cap \tilde{B}$ and $\widetilde{(A \cap B)} \leftrightharpoons \tilde{A} \cup \tilde{B}$ for all A and B.

(vi) $(\tilde{A} \cup B) \cap (A \cup \tilde{B}) \leftrightharpoons (A \cap B) \cup (\tilde{A} \cap \tilde{B})$.

[Remember (a) the principle of duality and (b) we have not yet introduced any relation $\subseteq$.]

4.5 *Introduction of the partial ordering* $\subseteq$

The set-inclusion relation $\subseteq$ on subsets is a relation which enables us to compare the relative sizes of certain pairs of subsets. Such relations in mathematics are called 'order relations' (or 'orderings') if they are applicable to any two elements (e.g., '$\leq$' between counting numbers is an order relation). If, as in our case, the relation is applicable to some pairs, but not to others, it is called a 'partial order relation' (or partial ordering). We introduce a partial ordering into our Boolean algebra by the following definition.

If A, B are elements of the algebra, we write $A \subseteq B$ (A is contained in B) when, and only when,

$$A \cup B \leftrightharpoons B.$$

Exercise 2. Show that the condition $A \cup B \leftrightharpoons B$ may be replaced by any one of the following conditions: $A \cap B \leftrightharpoons A$, $A \cap \tilde{B} \leftrightharpoons \varnothing$,

$\tilde{A} \cup B \leftrightharpoons U$, without destroying the analogy with the set relation 'is contained in'.

Exercise 3. (i) If $A \subseteq B$ and $B \subseteq A$, prove that $A \leftrightharpoons B$.

(ii) Show that, for all A, B: $A \cap B \subseteq A$, $A \cap B \subseteq B$, $A \subseteq A \cup B$, $B \subseteq A \cup B$ and $A \cap B \subseteq A \cup B$.

Exercise 4. (i) Show that, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$, i.e., $\subseteq$ is a transitive relation on the elements of the Boolean algebra.

(ii) Show that, if $A \subseteq B$, then $A \cup C \subseteq B \cup C$ and $A \cap C \subseteq B \cap C$ for all C.

Exercise 5. The relative complement of B with respect to A is denoted by $A-B$, where $A-B \leftrightharpoons A \cap \tilde{B}$. Prove that:

(i) $\tilde{A} \leftrightharpoons U-A$.

(ii) If $B \subseteq A$, $A-(A-B) \leftrightharpoons B$.

(iii) $(A-B)-C \subseteq A-(B-C)$ for all A, B, C.

(iv) $A-A \leftrightharpoons \emptyset$.

Exercise 6. (i) Show that $-$ is not commutative, and find the relation between A and B if $A-B \leftrightharpoons B-A$.

(ii) Is — associative? If $A \cap C \leftrightharpoons \emptyset$, find conditions on B for which $A-(B-C) \leftrightharpoons (A-B)-C$.

Exercise 7. (i) Show that:

(a) $A \cap (B-C) \leftrightharpoons A \cap B - A \cap C$;

(b) $(A \cap B)-C \leftrightharpoons (A-C) \cap (B-C)$;

and also that:

(c) $(A \cap B)-C \leftrightharpoons A \cap (B-C)$. What properties of $-$ do (a) and (b) reveal?

(ii) Show that $(A \cup B)-C \leftrightharpoons (A-C) \cup (B-C)$, and investigate whether $A \cup (B-C) \leftrightharpoons (A \cup B)-(A \cup C)$.

(iii) Find replacements for $A-(B \cup C)$ and $A-(B \cap C)$.

Exercise 8. The **symmetric difference**, $A+B$, of A and B is defined by $A+B \leftrightharpoons (A-B) \cup (B-A)$. Show that:

(i) $A+\emptyset \leftrightharpoons A$;

(ii) $A+U \leftrightharpoons \tilde{A}$;

(iii) $A+A \leftrightharpoons \emptyset$;

(iv) $A+B \leftrightharpoons \emptyset$ if and only if $A \leftrightharpoons B$;

(v) $A+B \leftrightharpoons A \cup B - A \cap B$.

Exercise 9. Prove that:

(i) $A+B \leftrightharpoons B+A$ for all A, B.
(ii) $A+(B+C) \leftrightharpoons (A+B)+C$ for all A, B, C.
(iii) If $C \leftrightharpoons A+B$ then $A \leftrightharpoons B+C$ and $B \leftrightharpoons A+C$.

Exercise 10. Show that:

(i) $A \cap (B+C) \leftrightharpoons (A \cap B)+(A \cap C)$.
(ii) $(A \cup B)+(A \cup C) \subseteq A \cup (B+C)$.

4.6 *Reducing the number of axioms*

We show now that axiom 4 (the associative laws) can be derived from the remaining axioms, so that, if we wish, we may delete it from the specifying conditions of the Boolean algebra.

By the principle of duality, we need establish one only of the associative laws. Let

$$X \leftrightharpoons A \cup (B \cup C) \quad \text{and} \quad Y \leftrightharpoons (A \cup B) \cup C.$$

We may use any of the remaining axioms, and any results deducible from the remaining axioms. In particular, we may use the results of §4.4, Ex. 1(iv):

$$A \cup (A \cap B) \leftrightharpoons A \quad \text{and} \quad A \cap (A \cup B) \leftrightharpoons A$$

if we can prove them without using axiom 4. We leave the reader to verify that the following is such a proof.

$$\begin{aligned} A &\leftrightharpoons A \cap U \\ &\leftrightharpoons A \cap (U \cup B) \\ &\leftrightharpoons (A \cap U) \cup (A \cap B) \\ &\leftrightharpoons A \cup (A \cap B). \end{aligned}$$

By duality, $A \leftrightharpoons A \cap (A \cup B)$.

We argue as follows:

$$\begin{aligned} A \cap X &\leftrightharpoons A \cap (A \cup (B \cup C)) \\ &\leftrightharpoons (A \cap A) \cup (A \cap (B \cup C)) \quad \text{by axiom 6} \\ &\leftrightharpoons A \cup (A \cap (B \cup C)) \\ &\leftrightharpoons A \end{aligned}$$

by the result just obtained.
Similarly we show $A \cap Y \leftrightharpoons A$.
Also,

$$\begin{aligned}\tilde{A} \cap X &\leftrightharpoons \tilde{A} \cap (A \cup (B \cup C))\\ &\leftrightharpoons (\tilde{A} \cap A) \cup (\tilde{A} \cap (B \cup C)) \quad \text{by axiom 6}\\ &\leftrightharpoons \emptyset \cup (\tilde{A} \cap (B \cup C))\\ &\leftrightharpoons \tilde{A} \cap (B \cup C).\end{aligned}$$

Similarly,

$$\tilde{A} \cap Y \leftrightharpoons \tilde{A} \cap (B \cup C).$$

Thus

$$A \cap X \leftrightharpoons A \cap Y, \quad \tilde{A} \cap X \leftrightharpoons \tilde{A} \cap Y.$$

Now

$$\begin{aligned}X &\leftrightharpoons X \cap U\\ &\leftrightharpoons X \cap (A \cup \tilde{A})\\ &\leftrightharpoons (X \cap A) \cup (X \cap \tilde{A})\\ &\leftrightharpoons (Y \cap A) \cup (Y \cap \tilde{A}) \quad \text{(by above)}\\ &\leftrightharpoons Y \cap (A \cup \tilde{A})\\ &\leftrightharpoons Y \cap U\\ &\leftrightharpoons Y.\end{aligned}$$

Hence $X \leftrightharpoons Y$, i.e., $A \cup (B \cup C) \leftrightharpoons (A \cup B) \cup C$.

In fact, it is possible to replace the present reduced axiom system by a different simpler system, but it is then quite a lengthy job to produce our present system of axioms. One example of this will be found in §7.5, Ex. 5 ($n(x, y)$).

4.7 *Summary*

We have been discussing the construction of an abstract mathematical system by the process of abstracting the relevant properties of a realisable system. The difficulties are many, but fall into two broad classes. Firstly, we have to recognise which properties of the real system are relevant to the analysis carried out on it, so that our initial premises or axioms can be properly and fully set down. Secondly, we have to force ourselves to abide by our self-imposed rules, and not to use some property not initially specified by us (but which perhaps exists in the real system)—i.e., we must train ourselves to think in terms of the symbols we are using.

We utilise the original real system by using the results we obtained in it as a guide to the possible results obtainable in our abstract system. That is, our intuitive understanding guides our reasoning processes into those directions where success seems likely. Sometimes we fail, and are led to explore our intuitive approach for errors. On the other hand, sometimes a result obtained by (apparently) unmotivated deduction will lead to a 'flash of insight'—a new way of perceiving not only our abstract system, but also the original, simple problem.

Sometimes an abstract system is formulated because it has been observed that several distinct real situations show a certain similarity, say in the pattern of operations involved, and it is desired to study a system where the extraneous dissimilar properties of each real system do not exist. On the other hand, one abstract system is often found to be applicable to some aspect or another of completely different real situations.

The abstract systems found in mathematics have mostly been developed in the way described above. There are however several important provisos. Firstly, by formulating a problem in abstract fashion, it has often been realised that a property one would not even dream of omitting in the real situation (because it happened, say, to be 'obvious' or 'part of our world') can be omitted, or even replaced by one flatly at variance with it, and the new set of premises still leads to an interesting abstract system, that is, one which is capable of producing many new results. In fact, the new, 'unreal' abstract systems sometimes turn out to be models of real situations! Such is the case with the most famous example: the rejection of Euclid's parallel axiom in plane geometry and its replacements with different postulates about parallel lines. Secondly, mathematicians sometimes see similarities between (what we would call) different abstract systems, and so are led to construct an abstract system which embraces the various systems previously developed.

We recommend that Chapters 5 and 6 of *Introduction to Set Theory and Logic* by R. R. Stoll, be read at this stage.

Chapter 5

H.C.F. AND L.C.M.

5.1 *Introduction*

In the first four chapters we have traced the evolution of a mathematical system (Boolean algebra) from a systematic study of the physical process of 'sorting'. The chapters which follow this one are to be devoted to the devising of other mathematical models which can be evolved from the same study. But in this chapter we pause a little to examine a sorting process which, within the structure of mathematics itself, is applied to the counting numbers. It is not the purpose of this book to analyse the structure of 'number' in the way that we have analysed the structure of 'sets'; we assume in fact that the reader is familiar with the ordinary axiomatic development of the system of counting numbers, and is satisfied that it is firmly based. The sorting process with which we are concerned is the factorisation of a counting number into its prime factors.

5.2 *Factorisation as a sorting process*

We assume that every positive number n can be expressed in a unique manner as the product of prime numbers. To find these numbers, we divide n by 2 as often as we can, obtaining a succession of numbers $\frac{1}{2}n$, $\frac{1}{4}n$, $\frac{1}{8}n$, . . . , $\frac{1}{2^r}n = n'$ the last of which, n' is odd. (It may be of course that n is odd, in which case $n' = n$, there being no factors 2.) Next we divide n' by 3 as often as possible to obtain a sequence $\frac{1}{3}n'$, $\frac{1}{9}n'$, . . . , n'', n'' being prime to 3; then successively as often as possible by 5, 7, 11, . . . until the final quotient is 1, that is, the preceding quotient is a prime. The number n is the product of all the divisors. For example:

$$10780 = 2 \times 5390$$

$$5390 = 2 \times 2695$$

2695 is not divisible by 3

$$2695 = 5 \times 539$$

$$539 = 7 \times 77$$

$$77 = 7 \times 11$$

$$11 = 11 \times 1.$$

$$10780 = 2.2.5.7.7.11.$$

We have in fact sorted out the factors of 10780.

Any counting number, then, determines a collection of prime numbers, namely, its prime factors. Since we have restricted the use of the term 'set' to a collection of objects which are all different, and since it is essential that we have to recognise, for example, two factors 2 and two factors 7 in the number 10780, we shall have to adopt some device which will enable us to include more than one of any factor in the set we are to construct.

In physical terms therefore let us suppose we have a set of cards, some of them marked 2, some marked 3, some 5, and so on. Let us now mark the cards '2' further by distinguishing them as 2_a, 2_b, 2_c, . . . , (and, if necessary 2_{aa}, 2_{ab}, . . . !), and mark similarly the cards '3' as 3_a, 3_b, 3_c, . . . , and similarly again the cards '5', '7', ... The subscripts *a*, *b*, *c*, . . . are without arithmetical significance, but later will be seen to play an essential part in the sorting process. We assume that we have in this pack at least as many cards marked with each number as are necessary for the problem on hand, but we do not at this stage contemplate discussing any such figment of the imagination as an 'infinite' pack of cards.

We now make the rule:

If a number n contains p^r (p prime) as a factor (but does not contain p^{r+1}) then we allocate to it the *first* r cards in the sequence of cards marked p_a, p_b, . . . (The word 'sequence' is used here in the same sense as 'ordered set', but again we attempt no definition.) Thus to the number 10780 we allocate the cards 2_a, 2_b, 5_a, 7_a, 7_b, 11_a.

In this way each counting number n that comes up for consideration is made to correspond to a set S_n of cards drawn from some given large enough set $\{2_a, 2_b, \dots 3_a, 3_b, \dots 5_a, 5_b, \dots\}$.

Thus

$$S_{10780} \simeq \{2_a, 2_b, 5_a, 7_a, 7_b, 11_a\},$$

$$S_{10920} \simeq \{2_a, 2_b, 2_c, 3_a, 5_a, 7_a, 13_a\},$$

$$S_{2640} \simeq \{2_a, 2_b, 2_c, 2_d, 3_a, 5_a, 11_a\}.$$

5.3 *The H.C.F. operation*

The most direct method of finding the Highest Common Factor of two numbers (though not usually the quickest) is to express each number in terms of its prime factors, and then to pick out all the common factors, a common factor which is repeated being counted as many times as it occurs in the set of common factors.

Consider the two numbers

$$\begin{array}{rccccccccc} 10780 = & 2. & 2. & & & 5. & 7. & 7. & 11, & \\ & \| & \| & & & \| & \| & & & \\ 10920 = & 2. & 2. & 2. & 3. & 5. & 7. & & & 13. \end{array}$$

If we compare this method of calculation with the definition of the sets S_{10780} and S_{10920} at the end of §2.2, and the definition of intersection, we see that

$$S_{10780} \cap S_{10920} \bumpeq \{2_a, 2_b, 5_a, 7_a\} \bumpeq S_{140}.$$

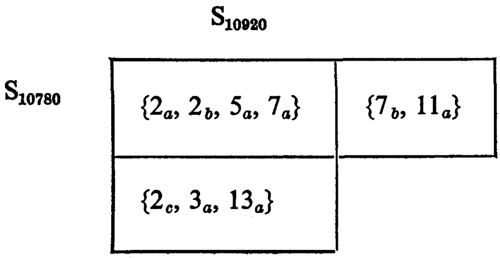
Now define the function $h(m, n)$ of two numbers m, n to be the Highest Common Factor of m and n, then the statements

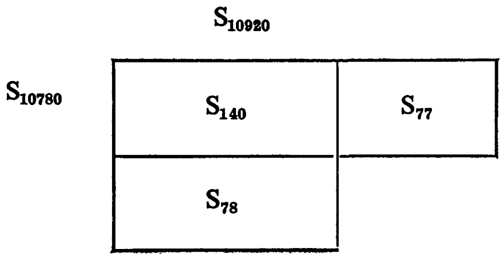
$$h(m, n) = k,$$

and $$S_m \cap S_n \bumpeq S_k$$

are equivalent. When $k = 1$, clearly $S_1 \bumpeq \varnothing$.

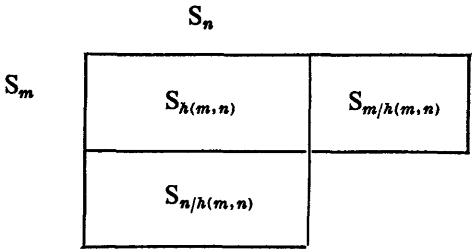
The corresponding Venn diagrams are





(The region corresponding to the intersection of the complements is left unmarked as being, in the present context, irrelevant: its marking depends on our initially selected set of indexed prime number cards, 2_a, 2_b, . . .)

For two general counting numbers m, n, the diagram is:



The primary subsets for the two-way dissections of S_m, S_n by the H.C.F. operation are

$$\begin{aligned} S_{h(m,n)} &\bumpeq S_m \cap S_n, \\ S_{m/h(m,n)} &\bumpeq S_m - S_{h(m,n)}, \\ S_{n/h(m,n)} &\bumpeq S_n - S_{h(m,n)}. \end{aligned}$$

We turn now to relations among three numbers; in particular consider 10780, 10920 and

$$2640 = 2.\ 2.\ 2.\ 2.\ 3.\ 5.\ 11.$$

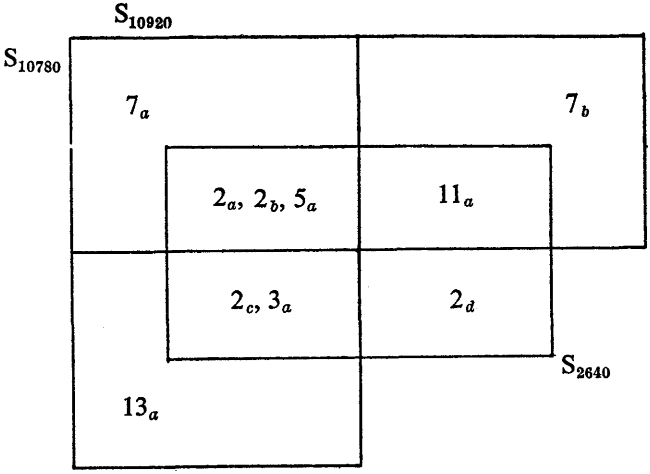
To find the H.C.F. of all three, we pick out the prime factors (repeated as necessary) common to all three numbers:

$$\begin{array}{rcccccccccc} 10780 & = & 2. & 2. & \ldots & \ldots & \ldots & 5. & 7. & 7. & 11, \\ & & \| & \| & & & & \| & & & \\ 10920 & = & 2. & 2. & 2. & . & 3. & 5. & 7. & \ldots & 13, \\ & & \| & \| & & & & \| & & & \\ 2640 & = & 2. & 2. & 2. & 2. & 3. & 5. & \ldots & \ldots & 11. \end{array}$$

The H.C.F. of the three numbers is $2.\ 2.\ 5 = 20$.
Again we can use the functional notation:

$$h(10780, 10920, 2640) = 20.$$

The corresponding Venn diagram is:



From this diagram we can see that, for these three numbers,

$$S_{h(k,\ m,\ n)} \hat{=} S_k \cap S_m \cap S_n.$$

5.4 *The L.C.M. operation*

The Least Common Multiple of the two numbers

10780 = 2. 2. . . . . . . 5. 7. 7. 11
10920 = 2. 2. 2. 3. 5. 7. 13

is the number which satisfies the conditions that it is the least number which contains all the prime factors of 10780 (since it is to be divisible by 10780) and all the prime factors of 10920. Thus it must contain factors

2. 2. 5. 7. 7. 11

(for 10780) and in addition

2. 3. 13

since these, with factors already in 10780, are those needed to give the product 10920. None of the nine factors listed can be omitted from the set of factors of any number which has as factors both 10780 and 10920, and the product of the nine factors is therefore the L.C.M. of the two numbers. But if we refer back to the first Venn diagram, we see that these are exactly the numbers which appear on the cards of the set $S_{10780} \cup S_{10920}$.

Thus, if we write $l(m, n)$ for the function of the two numbers m

and n of which the value is the L.C.M. of m and n, we see by reference to the third and fourth Venn diagrams in this chapter that, for these numbers

$$S_{l(m,\,n)} \mathrel{\hat{=}} S_m \cup S_n,$$

and

$$S_{l(k,\,m,\,n)} \mathrel{\hat{=}} S_k \cup S_m \cup S_n.$$

5.5 *Distributive relations*

Consider for the numbers $m = 10780$, $n = 10920$, $k = 2640$ the relations which correspond to the distributive relations. Take first

$$A \cup (B \cap C) \mathrel{\hat{=}} (A \cup B) \cap (A \cup C),$$

and consider the two corresponding factor expressions

$$l[m, h(n, k)] \quad \text{and} \quad h[l(m, n), l(m, k)].$$

$$\begin{aligned} l[m, h(n, k)] &= l(2.2.5.7.7.11, 2.2.2.3.5) \\ &= 2.2.2.3.5.7.7.11 \\ h[l(m, n), l(m, k)] &= h(2.2.2.3.5.7.7.11.13, 2.2.2.2.3.5.7.7.11) \\ &= 2.2.2.3.5.7.7.11. \end{aligned}$$

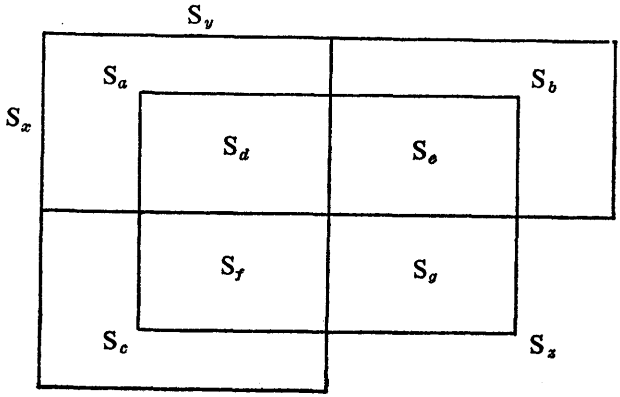
So that in this case

$$l[m, h(n, k)] = h[l(m, n), l(m, k)].$$

Exercise 1. Verify that in this case

$$h[m, l(n, k)] = l[h(m, n), h(m, k)].$$

Now let us analyse the relations and operations in terms of unspecified numbers corresponding to the primary subsets: suppose for the numbers x, y, z the Venn diagram takes the form



i.e.,

$$\begin{aligned} x &= abde \\ y &= acdf \\ z &= defg \\ h(x, y) &= ad. \end{aligned}$$

The two numbers be and cf can have no common factor since any such factor would provide an additional factor for the H.C.F. That is, be and cf are relatively prime, a relation which we shall write as

$$be \# cf.$$

We have, then,

$$\begin{array}{lll} h(x, y) = ad, & be \# cf, & l(x, y) = abcdef, \\ h(x, y) = de, & ab \# fg, & l(x, z) = abdefg, \\ h(y, z) = df, & ac \# eg, & l(y, z) = acdefg. \end{array}$$

Next $be \# cf \Rightarrow b \# c$, and $b \# f$, and $e \# c$, and $e \# f$, so that we have the following table of numbers which are relatively prime

	a	b	c	e	f	g
a	·			#	#	#
b		·	#		#	#
c		#	·	#		#
e	#		#	·	#	
f	#	#		#	·	
g	#	#	#			·

Any unmarked pair may have common factors, e.g., a and b, a and c, while d may have factors in common with any of the others. Because the necessary factors are relatively prime, we can prove the two associative properties:

$$\begin{aligned} h[h(x, y), z] &= h(ad, defg) = d \\ &= h[h(y, z), x] \\ l[l(x, y), z] &= l(abcdef, defg) = abcdefg \\ &= l[l(y, z), x]. \end{aligned}$$

In terms of these factors

$$l[x, h(y, z)] = l(abde, df) = abdef,$$

since f has no factor in common with abe.

$$h[l(x, y), l(x, z)] = h(abcdef, abdefg) = abdef,$$

since c and g have no common factor, so that corresponding to

$$\mathrm{S}_x \cup (\mathrm{S}_y \cap \mathrm{S}_z) \overset{\frown}{=} (\mathrm{S}_x \cup \mathrm{S}_y) \cap (\mathrm{S}_x \cup \mathrm{S}_z)$$

we have

$$l[x, h(y, z)] \equiv h[l(x, y), l(x, z)]$$

Exercise 2. Prove similarly that

$$l[h(x, y), h(x, z)] = h[x, l(y, z)].$$

5.6 *Complementation*

So far the properties of the operations of forming the H.C.F. and L.C.M. have been found to conform exactly with those of $\cap$, $\cup$, and we might suppose that the two systems are isomorphic (completely identical in structure). But we have not yet considered complementation; to avoid having to introduce a new number to complete the Venn diagram, we will consider only relative complementation (the operation of forming $\mathrm{A}-\mathrm{B}$).

We have defined the operation '+' by

$$\mathrm{A}+\mathrm{B} \overset{\frown}{=} (\mathrm{A}-\mathrm{B}) \cup (\mathrm{B}-\mathrm{A}),$$

and have proved that $(\mathrm{A}+\mathrm{B})+\mathrm{C} \overset{\frown}{=} \mathrm{A}+(\mathrm{B}+\mathrm{C})$ (§4.5). Corresponding to $\mathrm{A}-\mathrm{B}$ and $\mathrm{B}-\mathrm{A}$ we see from the diagram that we have the factors be and fc, which are relatively prime, so that, if we take

$$j(x, y) = l(x, y)/h(x, y)$$

to be the function corresponding to $\mathrm{A}+\mathrm{B}$:

$$\begin{aligned} j(x, y) &= bcef, \\ j(x, z) &= abfg, \\ j(y, z) &= aceg. \\ j(j(x, y), z) &= j(bcef, defg) = l(bcef, defg)/h(bcef, defg). \end{aligned}$$

We cannot go further than this, because we do not know whether d has any factors in common with bc.

To make the matter more precise, let us assume that, for any prime p, in x, y, z the highest powers of p are respectively p^r, p^s, p^t and that $r < s < t$ (this is only a matter of allocating the names x, y, z) and let us consider the actual power of p occurring in various functions:

$$\left.\begin{array}{ll} l(x, y) & : p^s \\ h(x, y) & : p^r \end{array}\right\} j(x, y) = \frac{l(x, y)}{h(x, y)} \ : \ p^{s-r}$$

$$\begin{aligned}
&j[j(x, y), z] &&: p^t/p^{s-r} = p^{t-s+r}\\
&\left.\begin{aligned}&l(y, z) &&: p^t\\ &h(y, z) &&: p^s\end{aligned}\right\} && j(y, z) = p^{t-s}\\
&j[j(y, z), x] &&: p^{t-s}/p^r \quad \text{or} \quad p^r/p^{t-s}\\
& &&= p^{t-s-r} \quad \text{or} \quad p^{r+s-t}, \quad \text{whichever power is positive.}
\end{aligned}$$

Thus in general

$$j[j(x, y), z] \neq j[j(y, z), x].$$

The situation is, then, that any operation on numbers involving the simple H.C.F. and L.C.M. processes follows exactly the pattern of the Boolean algebra of intersections and unions, but it is not possible to invent consistently an operation which corresponds to complementation.

Exercise 3. Prove the non-identity of the two forms above directly from the Venn diagram by expressing the numbers in the composite forms

$a = a'a''$, $b = b'b''$, $c = c'c''$, $e = e'e''$, $f = f'f''$, $g = g'g''$
$d = d'd''$, where $d'' = a''b''c''e''f''g''$, and all other pairs of numbers are relatively prime.

Exercise 4. Consider the set S_N where

$$N = 510510 = 2.3.5.7.11.13.17.$$

(i) Show that $S_1, S_2, \ldots, S_{17}$ can be taken to be the eight primary subsets of S_N under a three-way classification. Find three subsets S_x, S_y, S_z of S_N which determine a dissection of S_N into these eight primary subsets, and draw the corresponding Venn diagram.

(ii) Prove that if $S_n \subseteq S_N$ then $\widetilde{S}_n \bumpeq S_{N/n}$.

(iii) From your arrangement of the Venn diagram, prove that

$$j[j(x, y), z] = j[j(x, z), y]$$

and deduce that the corresponding relation holds for any three subsets of S_N.

(iv) Draw up a table of values of t (expressed in factors) for all sixteen subsets S_t of S_N determined by your choice of S_x, S_y.

Exercise 5. Outline an argument to show that if

$$N = p_0 p_1 \ldots p_r,$$

where $p_0, p_1, \ldots, p_r$ are $r+1$ different primes, then for any two subsets of $S_N \triangleq \{p_0, p_1, \ldots, p_r\}$, say

$$S_x \triangleq \{h_1, h_2, \ldots, h_i\} \subseteq \{p_0, p_1, \ldots, p_r\}$$
$$S_y \triangleq \{k_1, k_2, \ldots, k_j\} \subseteq \{p_0, p_1, \ldots, p_r\},$$

the operations $\sim$, $\cap$, $\cup$, $+$ correspond exactly to the operations of forming the numbers N/x (from x) and $h(x, y)$, $l(x, y)$, $j(x, y)$ (from x and y).

[A number such as N, which contains no repeated factors is referred to as a 'square-free number'.]

Chapter 6

SETS AND BINARY ARITHMETIC

6.1 *Twenty questions*

A game called 'Twenty Questions' is sometimes played on television; it is played by a chairman and a panel of four people acting as a team. At the opening of the session the chairman shows the viewers a placard (but does not let the members of the panel see it) on which is printed some such description as 'A duck swimming on Lake Burley Griffin' or 'President Johnson's ten-gallon hat'. With the object of discovering what was printed on the placard, the panel then asks the chairman twenty questions, to each of which he may answer only either 'Yes' or 'No'. There is no reason to doubt the genuineness of this performance, yet more often than not the panel manages to track down the object by the time it has had the answers to its twenty questions. Part of the reason for this success is undoubtedly some understanding of the chairman's pattern of thinking, part maybe is unconscious thought-transference from both the audience and the chairman to the members of the panel, but by far the greatest contribution to its success lies in the panel's ability to devise the right questions to ask, so that the members can eliminate as many classes of objects as possible from the need for further consideration. For instance, suppose the final answer is 'A duck swimming on Lake Burley Griffin': three or four questions could be expected to have narrowed down the field of inquiry to 'A member of the animal kingdom living in Australia'.

There are many much simpler versions of this same game, an example of which is the use of a simple device to track down the date of a friend's birthday. Suppose at first we are trying only to find the day of the week on which his next birthday falls. We show him cards on which are written the following lists of days, and he is asked to say on which of the lists the day appears:

I	II	III
Sunday	Monday	Wednesday
Tuesday	Tuesday	Thursday
Thursday	Friday	Friday
Saturday	Saturday	Saturday

(We see almost immediately that we could use three lists each of three days only; but we can develop the argument more easily on the basis of lists of four.) We can tabulate the possible answers thus:

	I	II	III
Sunday	Yes	No	No
Monday	No	Yes	No
Tuesday	Yes	Yes	No
Wednesday	No	No	Yes
Thursday	Yes	No	Yes
Friday	No	Yes	Yes
Saturday	Yes	Yes	Yes

It is then apparent that each day of the week corresponds to a different sequence of answers 'Yes' and 'No', and is consequently identifiable from these answers. If Saturday had been omitted, making three lists of three days each, we should have had three 'No' answers instead of three 'Yes', and the day would still have been identifiable.

To find the month of the birthday we need four cards, which could be marked:

I	II	III	IV
Jan.	Jan.	Jan.	Jan.
Mar.	Feb.	Feb.	Feb.
May	May	Mar.	Mar.
July	June	Apr.	Apr.
Sept.	Sept.	Sept.	May
Nov.	Oct.	Oct.	June
		Nov.	July
		Dec.	Aug.

Again the sequences of answers 'Yes' and 'No' for the cards in turn would be different for each month, and again we could have devised more economical lists than these. (See Exercise 1, p. 93).

Finally, to track down the date, we shall need five cards, which could be:

I	II	III	IV	V
1	2	4	8	16
3	3	5	9	17
5	6	6	10	18
7	7	7	11	19
9	10	12	12	20
11	11	13	13	21
13	14	14	14	22
15	15	15	15	23
17	18	20	24	24
19	19	21	25	25
21	22	22	26	26
23	23	23	27	27
25	26	28	28	28
27	27	29	29	29
29	30	30	30	30
31	31	31	31	31

(The '31' could be omitted, but apart from this reduction, there is no more economical set of lists.)

6.2 *Labelling by binary numbers*

The last set of lists provides the key to the actual process that we have been following in constructing the lists. Effectively, we have numbered the days of the week 1 to 7, the months of the year 1 to 12, and the days of the month 1 to 31, and have then expressed each of the numbers in the binary scale. For example, in the case of the days of the week we have:

Day	Number	Reversed binary notation units 2's 4's
Sunday	1 = 1+0+0	(1, 0, 0)
Monday	2 = 0+2+0	(0, 1, 0)
Tuesday	3 = 1+2+0	(1, 1, 0)
Wednesday	4 = 0+0+4	(0, 0, 1)
Thursday	5 = 1+0+4	(1, 0, 1)
Friday	6 = 0+2+4	(0, 1, 1)
Saturday	7 = 1+2+4	(1, 1, 1)

The 1's and 0's correspond exactly to the 'Yes's' and 'No's' in the previously constructed identifying table. So that, given for example the successive answers Yes, No, Yes for tables I, II, III, we know at once that the day required is the n-th where $n = 1+0+4 = 5$, that is, it is the fifth day, Thursday.

The reader should notice that we have used the *reversed* binary representation of the number, namely,

$$n = u_1 + u_2 \times 2 + u_3 \times 4 + \ldots + u_r \times 2^{r-1},$$

and written this as $(u_1, u_2, u_3, \ldots, u_r)$. The usual way of writing the same number on the binary scale is

$$n = u_r u_{r-1} \ldots u_3 u_2 u_1 = u_r \times 2^{r-1} + u_{r-1} \times 2^{r-2} + \ldots + u_3 \times 4 + u_2 \times 2 + u_1.$$

The way we have written the number is that which arises more naturally in this context, and is much the more convenient for the various purposes for which we propose to use it.

The effect of preparing the lists of days, months and dates is to separate the elements of the universal set concerned into subsets and their complements in such a way that each element by itself forms a primary subset (leaving some of the primary subsets empty). We can clearly analyse any dissection of a set into subsets in a corresponding way whether or not we wish to reduce it ultimately to a state in which each element individually forms a primary subset.

Let us look again at the days of the week in this light. Take

A ≏ {Sunday, Tuesday, Thursday, Saturday}
Ã ≏ {Monday, Wednesday, Friday}
B ≏ {Monday, Tuesday, Friday, Saturday}
B̃ ≏ {Sunday, Wednesday, Thursday}.

On the Venn diagram these would be tabulated thus:

	B	B̃
A	Tue. Sat.	Sun. Thur.
Ã	Mon. Fri.	Wed.

If we were not going further with the classification, we could now label the primary subsets on this table thus:

Tue., Sat.	(1, 1)	or	1+2	or	3	
Sun., Thur.	(1, 0)	or	1+0	or	1	
Mon., Fri.	(0, 1)	or	0+2	or	2	
Wed.	(0, 0)	or	0+0	or	0.	

That is, the labels are:

	B	$\tilde{B}$
A	(1, 1)	(1, 0)
$\tilde{A}$	(0, 1)	(0, 0)

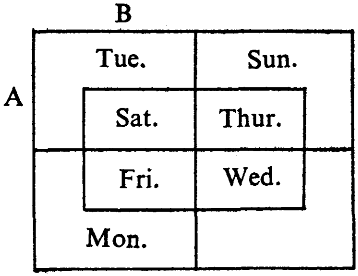
or

[3]	[1]
[2]	[0]

and $A \bumpeq \{[3], [1]\}^* \bumpeq \{\text{Tue., Sat.; Sun., Thur.}\}$

$B \bumpeq \{[3], [2]\} \bumpeq \{\text{Tue., Sat.; Mon., Fri.}\}$.

In the next classification, (which in this case, identifies the elements completely) we change from the four binary numbers, 0+0 to 1+2, to the eight binary numbers, 0+0+0 to 1+2+4, by adding 4 to the present number which corresponds to an element falling in the new classification and leaving the others unchanged. That is, first the new Venn diagram appears as:



---

*We have in effect extended the use of the notation $\{a, b, c, \ldots\}$ for listing the members of a set, in that [1] and [3] are not members of the set but lists of members (i.e., subsets of the set), having the essential property that they have no common members, $[1] \cap [3] \bumpeq \emptyset$. There are in fact two other ways in which the set represented by {[1], [3]} could be represented, namely, as

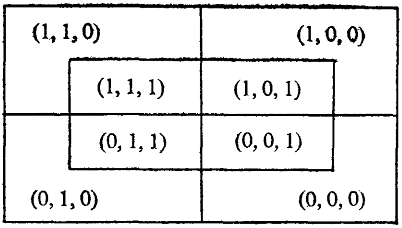
$$[1] \cup [3]$$

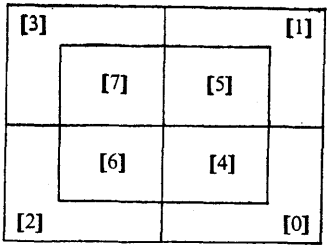
or, since $[1] \cap [3] \bumpeq \emptyset$, as

$$[1] + [3],$$

of which the second is usually the more appropriate. However, in the present context the form {[1], [3]} seems to have most to recommend it.

and then in the successive forms:





leading us back to the list we had on p. 90.

Exercise 1. By selecting an appropriate set of 12 sequences (ordered sets) of four numbers each 0 or 1, show that four lists each of five months are sufficient to identify a month.

Exercise 2. Devise the most economical type of set of lists for identifying

(i) the 26 letters of the alphabet;
(ii) the 52 cards of a pack.

Let us apply this process to the subdivision of the class of children that we have used as our basic example. In our earlier discussion we have imagined each child provided with a label on which is written 'G' if the child is a girl, 'L' if the child is left-handed, and 'S' if the child wears spectacles, or '$\tilde{\mathrm{G}}$', '$\tilde{\mathrm{L}}$', '$\tilde{\mathrm{S}}$' respectively if the child does not conform to these descriptions. Now replace the label by another on which we write '1' when the child conforms to a description and '0' when he does not. So long as we used the different letters 'G', 'L', 'S' the order in which we applied the classifications has not been relevant: to state of a given element k,

$$k \in \mathrm{G} \cap \tilde{\mathrm{L}} \cap \mathrm{S},$$

conveys exactly the same meaning as stating

$$k \in \tilde{\mathrm{L}} \cap \mathrm{G} \cap \mathrm{S} \quad \text{or} \quad k \in \mathrm{S} \cap \mathrm{G} \cap \tilde{\mathrm{L}}.$$

But if we are going to use only '1's' and '0's' we must make it clear to which classification each digit refers.

That is, we lay down an order of classifications, say G followed by L followed by S, so that if

$k \in \mathrm{G}$, then the *first* digit on the label is 1

$k \in \tilde{\mathrm{G}}$, ,, ,, *first* ,, ,, ,, ,, ,, 0

$k \in \mathrm{L}$,, ,, *second* ,, ,, ,, ,, ,, 1

$k \in \tilde{\mathrm{L}}$, ,, ,, *second* ,, ,, ,, ,, ,, 0

$k \in \mathrm{S}$, ,, ,, *third* ,, ,, ,, ,, ,, 1

$k \in \tilde{\mathrm{S}}$, ,, ,, *third* ,, ,, ,, ,, ,, 0.

Briefly, while the labels (G, $\tilde{\mathrm{L}}$, S), (S, $\tilde{\mathrm{L}}$, G), (S, G, $\tilde{\mathrm{L}}$), . . . may all equally well be attached to elements of the same subset, once the order of the classifications has been fixed as S, L, G, then the only 'binary' label that can be attached to an element of that subset is (1, 0, 1).

With this notation we can allow for any number r of classifications, giving rise to subsets $\mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_r$ and their complements: we specify an order in which the classifications are to be applied, and then attach to each element k of the set,

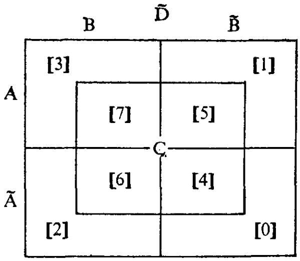
(i) a label $(u_1, u_2, \ldots, u_r)$, where

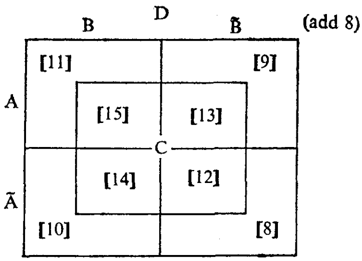
$$u_i = 1 \quad \text{if } k \in \mathrm{P}_i$$
$$u_i = 0 \quad \text{if } k \in \tilde{\mathrm{P}}_i, \quad \text{and then}$$

(ii) a label $[n]$, where $n = u_1 + 2u_2 + 4u_3 + 8u_4 + \ldots + 2^{r-1}u_r$.

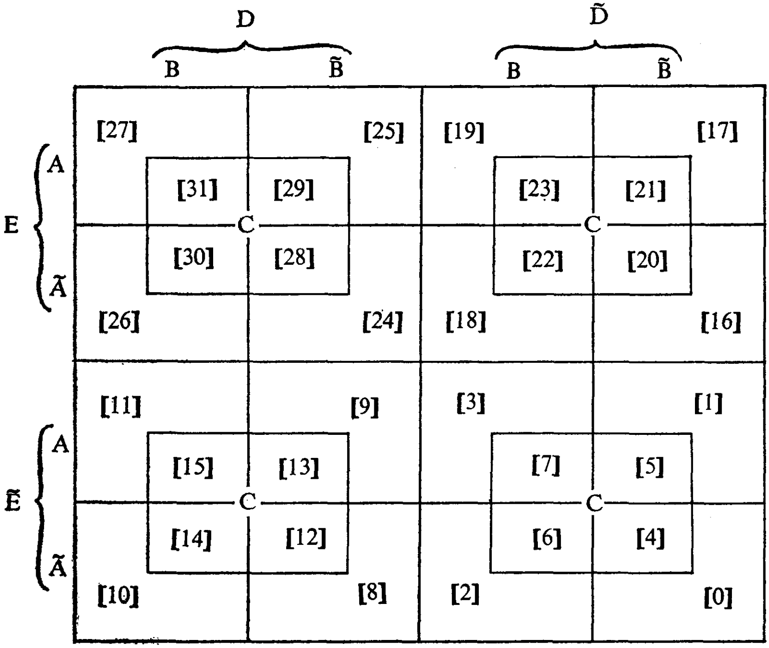
All elements bearing the same label $[n]$ belong to the same primary subset.

We have already drawn the Venn diagrams for two and three classifications. For four classifications we could draw two complementary diagrams:





The quintuple diagram we could put together in the form:



But a more compact and revealing tabulation is a simple arrangement of the 32 lists and the classification to which each belongs.

0					(0,0,0,0,0)
1	A				(1,0,0,0,0)
2		B			(0,1,0,0,0)
3	A	B			(1,1,0,0,0)
4			C		(0,0,1,0,0)
5	A		C		(1,0,1,0,0)
6		B	C		(0,1,1,0,0)
7	A	B	C		(1,1,1,0,0)
8				D	(0,0,0,1,0)
9	A			D	(1,0,0,1,0)
10		B		D	(0,1,0,1,0)
11	A	B		D	(1,1,0,1,0)
12			C	D	(0,0,1,1,0)
13	A		C	D	(1,0,1,1,0)
14		B	C	D	(0,1,1,1,0)
15	A	B	C	D	(1,1,1,1,0)

16					E	(0,0,0,0,1)
17	A				E	(1,0,0,0,1)
18		B			E	(0,1,0,0,1)
19	A	B			E	(1,1,0,0,1)
20			C		E	(0,0,1,0,1)
21	A		C		E	(1,0,1,0,1)
22		B	C		E	(0,1,1,0,1)
23	A	B	C		E	(1,1,1,0,1)
24				D	E	(0,0,0,1,1)
25	A			D	E	(1,0,0,1,1)
26		B		D	E	(0,1,0,1,1)
27	A	B		D	E	(1,1,0,1,1)
28			C	D	E	(0,0,1,1,1)
29	A		C	D	E	(1,0,1,1,1)
30		B	C	D	E	(0,1,1,1,1)
31	A	B	C	D	E	(1,1,1,1,1)

For two, three and four classifications we use the table as far respectively as the lines marked 3, 7 and 15. Formally, the numbers corresponding to the various subsets are

$$\begin{array}{lll}
\mathrm{A} : \{[a] & : a & = 1+2y+4z+8t+16u+\ldots\} \\
\tilde{\mathrm{A}} : \{[a'] & : a' & = 0+2y+4z+8t+16u+\ldots\} \\
\mathrm{B} : \{[b] & : b & = x+2+4z+8t+16u+\ldots\} \\
\tilde{\mathrm{B}} : \{[b'] & : b' & = x+0+4z+8t+16u+\ldots\} \\
\mathrm{C} : \{[c] & : c & = x+2y+4+8t+16u+\ldots\} \\
\tilde{\mathrm{C}} : \{[c'] & : c' & = x+2y+0+8t+16u+\ldots\} \text{ etc.}
\end{array}$$

where in each set the symbol $[n]$ takes the values obtained by giving $x, y, z, t, u, \ldots$ all possible combinations of values 0, 1.

6.3 *Binary numbers and the characteristic sequences*

The question could now be raised, can this representation of the subsets be used, on a suitable axiomatic basis, to prove the fundamental relations involving the set operations? If we had to consider in any of these operations an unspecified number of classifications the arithmetical complications might make the attempt to do this not worth while. But, in fact, the whole basis of set-algebra is laid down when we have described the relations for three classifications.

A formal statement then could be the following:

$\mathrm{U} \mathrel{\hat{=}} \{\ldots, k, \ldots\}$ (k is a representative member of U)
$\mathrm{A} \subset \mathrm{U}, \mathrm{B} \subset \mathrm{U}, \mathrm{C} \subset \mathrm{U}.$

To each k assign a sequence (x, y, z) of three digits, each 0 or 1, in the following way

$$\begin{aligned} k \in \mathrm{A} &\Leftrightarrow x = 1\,;\; k \in \tilde{\mathrm{A}} \Leftrightarrow x = 0,\\ k \in \mathrm{B} &\Leftrightarrow y = 1\,;\; k \in \tilde{\mathrm{B}} \Leftrightarrow y = 0,\\ k \in \mathrm{C} &\Leftrightarrow z = 1\,;\; k \in \tilde{\mathrm{C}} \Leftrightarrow z = 0. \end{aligned}$$

This sequence we shall call the 'characteristic sequence' of the subset.

Form the sums $n = x+2y+4z$. Denote by $[n]$ the subset of elements of U for which $x+2y+4z = n$. Then*

$$\begin{aligned} \mathrm{A} &\bumpeq \{[n] : n = 1+2y+4z, y = 0, 1, z = 0, 1\}\\ &\bumpeq \{[1], [3], [5], [7]\},\\ \tilde{\mathrm{A}} &\bumpeq \{[n] : n = 0+2y+4z, y = 0, 1, z = 0, 1\}\\ &\bumpeq \{[0], [2], [4], [6]\},\\ \mathrm{B} &\bumpeq \{[2], [3], [6], [7]\},\\ \tilde{\mathrm{B}} &\bumpeq \{[0], [1], [4], [5]\},\\ \mathrm{C} &\bumpeq \{[4], [5], [6], [7]\},\\ \tilde{\mathrm{C}} &\bumpeq \{[0], [1], [2], [3]\}. \end{aligned}$$

The commutation and association properties are immediate deductions. We have also

$$\mathrm{A} \cup \mathrm{B} \bumpeq \{[1], [2], [3], [5], [6], [7]\}$$

so that

$$\begin{aligned} \tilde{\mathrm{A}} \cap \tilde{\mathrm{B}} &\bumpeq \{[0], [4]\} \bumpeq \widetilde{\mathrm{A} \cup \mathrm{B}}.\\ \mathrm{A}-\mathrm{B} &\bumpeq \{[1], [3], [5], [7]\}-\{[2], [3], [6], [7]\}\\ &\bumpeq \{[1], [5]\}.\\ \mathrm{A}\,\sigma\,\mathrm{B} &\bumpeq \{[0], [2], [4], [6]\} \cup \{[2], [3], [6], [7]\}\\ &\bumpeq \{[0], [2], [3], [4], [6], [7]\}. \end{aligned}$$

Exercise 3. Use the above dissections of the subsets to prove:

(i) $\mathrm{A} \cup (\mathrm{B} \cap \mathrm{C}) \bumpeq \{[1], [3], [5], [6], [7]\} \bumpeq (\mathrm{A} \cup \mathrm{B}) \cap (\mathrm{A} \cup \mathrm{C})$.

(ii) $(\mathrm{A}\,\sigma\,\mathrm{B}) \cap (\mathrm{B}\,\sigma\,\mathrm{C}) \subseteq \mathrm{A}\,\sigma\,\mathrm{C}$.

(iii) $\mathrm{A}-(\mathrm{B} \cap \mathrm{C}) \bumpeq (\mathrm{A}-\mathrm{B}) \cup (\mathrm{A}-\mathrm{C})$.

(iv) $(\mathrm{A} \cup \mathrm{B}) \cap (\mathrm{C} \cup \mathrm{D}) \bumpeq (\mathrm{A} \cap \mathrm{C}) \cup (\mathrm{A} \cap \mathrm{D}) \cup (\mathrm{B} \cap \mathrm{C}) \cup (\mathrm{B} \cap \mathrm{D})$.

Exercise 4. Express as compactly as possible the subset

$$(\mathrm{P}_1 \cap \mathrm{P}_2) \cup (\mathrm{P}_3 \cap \mathrm{P}_4) \cup (\mathrm{P}_5 \cap \mathrm{P}_6)$$

as the union of a set of primary subsets.

---

*It should be recognised that we are using the sum $[n]$ only as a compact way of representing the characteristic sequence, e.g., [5] for (1, 0, 1).

6.4 *The index number of a subset*

The primary subsets, $[n]$, are disjoint, and any subset of U (including U itself) can be constituted in a unique way as the union of primary subsets. For two classifications the whole set of subsets of U consists of:

$\emptyset$ 1

primary subsets, $[3] \bumpeq A \cap B$, $[2] \bumpeq \tilde{A} \cap B$ 4
$[1] \bumpeq A \cap \tilde{B}$, $[0] \bumpeq \tilde{A} \cap \tilde{B}$

unions of two primary subsets, namely,
$A, B, \tilde{A}, \tilde{B}, A+B, \widetilde{A+B}$ 6

unions of three primary subsets, namely, 4
$A \cup B, A \cup \tilde{B}, \tilde{A} \cup B, \tilde{A} \cup \tilde{B}$

U 1,

altogether $16 = 2^4$ including $\emptyset$ and U.

For r classifications there are 2^r primary subsets, corresponding to the 2^r characteristic sequences $(u_1, u_2, \ldots, u_r)$, $u_i = 0$ or 1, and represented by the symbols $[n]$, where $n = u_1+2u_2+ \ldots +2^{r-1}u_r$. Since any subset P of U is a union of members of the set of primary subsets, it can be represented by a sequence $(w_0, w_1, \ldots, w_{2^r-1})$, where $w_i = 1$ if $P \supseteq [i]$, and $w_i = 0$ if $P \cap [i] \bumpeq \emptyset$. Thus, for a given dissection of U by r classifications, if none of the primary subsets is empty, there are $(2)^{2^r}$ distinct subsets of U, to each of which may be attached a distinctive index number N, where

$$N = w_0+2w_1+ \ldots +2^{(2^r-1)}w_{2^r-1}.$$

The index numbers of the primary subsets are $1, 2, 4, \ldots, 2^r-1$. The index numbers of the sixteen subsets under a two-way classification are shown on the next page.

For three classifications, there are 256 distinct subsets (including $\emptyset$ and U); for example

$$A \cup (B \cap C) \bumpeq \{[1], [3], [5], [6], [7]\}$$

is represented by the sequence (0,1,0,1,0,1,1,1), and has the index number $N = 2^1+2^3+2^5+2^6+2^7 = 234$.

While this could be used as a method of labelling the subsets of a set under given classifications, in the next chapter we shall devise a much more powerful way of employing the characteristic sequences that we have used as labels for the primary subsets.

Subset	Constituent primary subsets	w-sequence	Index numbers
$\emptyset$			0
$A \cap B$	[3]	(0,0,0,1)	8
$A-B$	[1]	(0,1,0,0)	2
$B-A$	[2]	(0,0,1,0)	4
$\widetilde{A \cup B}$	[0]	(1,0,0,0)	1
A	[1], [3]	(0,1,0,1)	10
$\tilde{A}$	[0], [2]	(1,0,1,0)	5
B	[2], [3]	(0,0,1,1)	12
$\tilde{B}$	[0], [1]	(1,1,0,0)	3
$A+B$	[1], [2]	(0,1,1,0)	6
$\widetilde{A+B}$	[0], [3]	(1,0,0,1)	9
$A \cup B$	[1], [2], [3]	(0,1,1,1)	14
$A \sigma B$	[0], [2], [3]	(1,0,1,1)	13
$B \sigma A$	[0], [1], [3]	(1,1,0,1)	11
$\widetilde{A \cap B}$	[0], [1], [2]	(1,1,1,0)	7
U	[0], [1], [2], [3]	(1,1,1,1)	15

Exercise 5. By expressing the index numbers 234 and 178 of two subsets in binary form, find the index numbers of their intersection and union. Verify your answers by reference to regions on the Venn diagram.

Exercise 6. A set is divided into 2^{r-1} primary subsets by $r-1$ classifications. A certain subset Q is the union of the k primary subsets $[n_i]$, $i = 1, \ldots, k$. A further classification is introduced producing subsets R and $\tilde{R}$, and the whole set of 2^r primary subsets is now listed. Prove that

$$Q \cap R \bumpeq \{[n_i'] : n_i' = 2^{r-1}+n_i\}$$

$$Q \cap \tilde{\tilde{R}} \bumpeq \{[n_i]\}.$$

(Compare first the diagrams on pp. 93-95 for three, four and five classifications.)

Exercise 7. Prove that, A, B, C, . . . being the subsets that determine the dissection,

(i) $A+B+C \doteqdot \{[1], [2], [4], [7]\}$

(ii) $A+B+C+D \doteqdot \{[1], [2], [4], [8], [14], [13], [11], [7]\}$

(iii) (by induction)

$$A_1+A_2+\ldots+A_r \doteqdot \{[n]: n = u_1+2u_2+\ldots+2^{r-1}u_r, \text{ and } u_1+u_2+\ldots+u_r \text{ is odd.}\}$$

Exercise 8. In a dissection by two subsets the index sequences of two subsets F and G are (u_0, u_1, u_2, u_3) and (v_0, v_1, v_2, v_3). Prove the index sequence of F+G is $(u_0+v_0, u_1+v_1, u_2+v_2, u_3+v_3)$, where u_i+v_i is replaced by 0 when $u_i = v_i = 1$.

Sketch a proof of the corresponding theorem for a dissection by r subsets, and discuss Exercise 7 in the light of this result.

Chapter 7

SETS AND BINARY ALGEBRA

7.1 *The analogy with Cartesian Geometry*

The device of assigning characteristic sequences of indices each 1 or 0 to the elements of a set according as they do or do not satisfy various descriptions, while it may have helped to clarify the picture of set relations, did not seem to lead to a satisfactory mathematical model, in the sense that we were still left with the necessity for visual verification, and could not write down recognisable mathematical formulae and identities.

We look therefore for ways of manipulating these sequences of 1's or 0's other than those which follow from treating the elements of the sequence as the digits forming a number expressed in the binary scale.

One possible line of development is that of treating the digits in a sequence as a set of 'co-ordinates' analogous to 'Cartesian co-ordinates' which are used to identify points in a plane (or space of three or more dimensions). There is of course the essential difference that the 'co-ordinates' derived from the characteristic sequence of a member of a set take only the values 0 and 1, and the identification is usually much less precise, in the sense that all members of the same primary subset have the same 'co-ordinates'.

Let us consider the analogy in the case where there are only two relevant classifications, and the primary subsets are $A \cap B$, $A \cap \tilde{B}$, $\tilde{A} \cap B$, $\tilde{A} \cap \tilde{B}$, corresponding to the characteristic sequences (1,1), (1,0),(0,1),(0,0). In writing (x_k, y_k) for the pair corresponding to the member k of U for the sequence, we mean that the value of $\left\{\begin{matrix} x_k \\ y_k \end{matrix}\right.$ determines the relation of k to the subset $\left\{\begin{matrix} \mathrm{A} \\ \mathrm{B} \end{matrix}\right.$, i.e, either $\left\{\begin{matrix} k \in \mathrm{A} \text{ or } k \notin \mathrm{A} \\ k \in \mathrm{B} \text{ or } k \notin \mathrm{B} \end{matrix}\right.$. Correspondingly: In writing (x_k, y_k) for the co-ordinate-pair of a point k of the Cartesian plane, we mean that the value of $\left\{\begin{matrix} x_k \\ y_k \end{matrix}\right.$ determines the relation of k to the line $\left\{\begin{matrix} \alpha(\text{the } y\text{-axis}) \\ \beta(\text{the } x\text{-axis}) \end{matrix}\right.$, namely $\left\{\begin{matrix} x_k \\ y_k \end{matrix}\right.$ is the distance of the point from $\left\{\begin{matrix} \alpha \\ \beta \end{matrix}\right.$.

The entities in the set-algebra that correspond exactly to the points in the plane are the primary subsets (relative to the given classifications). While all points of the plane are regarded as different, no distinction is made among the members of U which, for any given system of classifications, are members of the same primary subset.

Let us analyse a little further what we have been doing in relation to the set and the geometry. In the geometry we have a set of distances, x, along a line.* From this we construct a new set of pairs of distances x, y from two (perpendicular) lines; if we were investigating geometry in three dimensions, we should construct a set of sequences of three distances x, y, z from three mutually perpendicular planes.

Correspondingly, in analysing the universal set, from the set $\{1, 0\}$ we construct the set $\{(x, y)\}$ of ordered pairs (x, y) for a two-way classification, the set of ordered triples (x, y, z) for a three-way classification and so on.

This process of forming new sets, by forming sequences whose elements are members of given sets (which need not be all the same) is of frequent application in mathematics, and because of the prototype in Cartesian Geometry, it is called the 'Cartesian product' set.

Given any sets A, B, with typical members $a \in \mathrm{A}$, $b \in \mathrm{B}$, the set of ordered pairs $\{(a, b)\}$ is the Cartesian product, written $A \times \mathrm{B}$.

The product may be extended to any number of terms, thus

$\mathrm{A} \times \mathrm{B} \times \mathrm{C} \times \ldots \bumpeq \{(a, b, c, \ldots) : a \in \mathrm{A}, b \in \mathrm{B}, c \in \mathrm{C}, \ldots\}$.

In the sense in which we shall always need to use the name 'Cartesian product', the product is not commutative: $\mathrm{A} \times \mathrm{B} \not\bumpeq \mathrm{B} \times \mathrm{A}$, for while it is conceivable that, because of the associations of the particular letters, (x, y) and (y, x) might sometimes be regarded as the same point, it is quite certain that $(1, 2)$ and $(2, 1)$ may not. We shall in fact regard a Cartesian product as a set of sequences, each element of a sequence being drawn usually from the same set, but cases of different sets also come up for discussion.

In the Cartesian Geometry a relation, say $lx+my+n = 0$, connecting the co-ordinates x and y serves to pick out from the plane those points which lie on some 'locus', in the particular case referred to above, a 'line'. In the same way, a relation between the two components of the characteristic sequences (x, y) of members of the set U defines a subset of U to which all members belong whose characteristic sequences satisfy the relation.

---

*This is a type of set (a non-finite set) that we do not discuss until Chapter 9, but we do not use here any of the ideas involved except by way of illustration.

Just as Cartesian (analytical) Geometry is a 'mathematical model' for Euclidean Geometry and hence ultimately for physical geometry, so this analogous structure that we are aiming to establish will be a mathematical model for the algebra of intersections and unions of sets, and hence for the physically observable relations among subsets.

7.2 *Binary algebra*

We have to draw up the rules for the combination of the 1's and 0's of a characteristic sequence which correspond to the rules for addition and multiplication of the numbers of ordinary arithmetic that form the basis for analytical geometry. One such set of rules are those of Boolean algebra to which we refer later (§7.8). Our immediate concern is with the rules of 'binary algebra' which are in fact the rules for addition and multiplication of the counting numbers applied in the situation where we require to know of a number only whether it is odd or even.

Just as in discussing set relations, we needed two forms of the sign '=' to correspond to the two distinct meanings, namely,

$\bumpeq$ 'is the same set as' when the relation is explicitly between sets,

$\leftrightarrows$ 'may be replaced by' when the relation is between symbols, so here we need altogether three different signs, any of which, when the meanings have become familiar, may be replaced by =. Let $f(x, y)$ and $g(x, y)$ be functions of x and y in the binary algebra (we see shortly that the most general such function is $a+bx+cy+dxy$); the three meanings are represented by the symbols:

$=$: $f(x, y) = 0$; this is an equation which is satisfied by certain pairs of values (x, y), the 'solutions' of the equation.

$\equiv$: $f(x, y) \equiv g(x, y)$; the functions f and g take the same values for every pair (x, y), in fact, written in their simplest forms f and g correspond exactly term by term.

$\boldsymbol{=}$: $f(x, y) \boldsymbol{=} 0$; the system we are concerned with is such that the only admissible values (x, y) are those for which $f(x, y) \boldsymbol{=} 0$. In other words, the system is such that there are no elements in the set with characteristic sequence for which $f(x, y) = 1$. For example, we discuss in §7.4 the dissection of U by a pair of subsets which are such that $A \subseteq B$, i.e., such that $A \cap \tilde{B} \bumpeq \varnothing$, and there are no elements in U with characteristic sequence $(1, 0)$.

Axioms for binary algebra: The algebra contains only two elements, 1, 0, and two operations for combining pairs of elements, +, ×, the whole system of combinations being prescribed in the tables

$x+y$:

$x \diagdown y$	1	0
1	0	1
0	1	0

$x \times y$:

$x \diagdown y$	1	0
1	1	0
0	0	0

These form the complete set of axioms. From them we deduce immediately from the symmetry of the tables

T 1. '+' and '×' are both commutative operations.

T 2. '+' and '×' are both associative.

Proof: (i) $a+(b+c)$ and $(a+b)+c$

$b = 0$: $a+(0+c) = a+c = (a+0)+c$

$b = 1, a = c$: $a+(1+a) = (a+1)+a$

by two applications of T 1.

$b = 1, a = 0, c = 1$: $0+(1+1) = 0 = (0+1)+1$

$a = 1, c = 0$: $1+(1+0) = 0 = (1+1)+0$;

(ii) $a\times(b\times c)$ and $(a\times b)\times c$

$b = 0$: $a\times(0\times c) = a\times 0 = 0 = (a\times 0)\times c$

$b = 1$: $a\times(1\times c) = a\times c = (a\times 1)\times c$.

T 3. '×' is distributive over '+'.

Proof: $a\times(b+c)$ and $(a\times b)+(a\times c)$

$a = 0$: $0\times(b+c) = 0 = (0\times b)+(0\times c)$

$a = 1$: $1\times(b+c) = b+c = (1\times b)+(1\times c)$.

T 4. '+' is not distributive over '×'.

Exercise: Prove this by finding a counter-example.

Another particular consequence of the axioms is

T 5. $x^2 \equiv x$

so that $x^3 \equiv x\times x^2 \equiv x\times x \equiv x$

$x^4 \equiv x\times x^3 \equiv x\times x \equiv x$ etc.

Since $x+x \equiv 0$, we may write

$$x^2+x \equiv 0$$

and may frequently shorten algebra by using this relation.

In practice, we shall use the ordinary method of writing

$$xy \quad \text{or} \quad x.y$$

for $\quad x \times y,$

and $\quad xy+z$ for $(x \times y)+z$ etc.,

since no ambiguity is introduced.

7.3 *Binary algebra and set operations*

We repeat (from the last chapter) the rules which determine the method by which the marks 0, 1 are to be applied to the sets. Let the members of the set be listed by subsets $A_1, A_2, \ldots, A_n$ and their complements $\tilde{A}_1, \ldots, \tilde{A}_n$; assign to each member k of the set its characteristic sequence $(x_1, \ldots, x_n)$ in which

$$k \in A_i \Leftrightarrow x_i = 1$$
$$k \in \tilde{A}_i \Leftrightarrow x_i = 0.$$

Our aim is to devise functions of the elements of the sequence corresponding to the various set operations, which take the values 1 or 0 when the members do or do not belong to the subset determined by the operation. We need of course to consider in any particular theorem only as many of the subsets $A_1, A_2, \ldots$ as are necessary to state the theorem, and shall use, as we have done previously, A, B, C, . . . , for the names of the subsets and $(x, y, z, \ldots)$ for the characteristic sequence.

Complementation $\tilde{A}$: The function $c(x)$, corresponding to complementation, has to conform to the conditions:

$$k \in \tilde{A} \quad \text{when} \quad x = 0, \quad \text{i.e.,} \quad c(0) = 1$$
$$k \in \tilde{\tilde{A}} \bumpeq A \quad \text{when} \quad x = 1, \quad \text{i.e.,} \quad c(1) = 0.$$

The only function with this property is

$$c(x) \equiv 1+x,$$

and we note that $c\{c(x)\} \equiv 1+(1+x) \equiv x$.
We define therefore

$$c(x) \overset{\text{def}}{=} 1+x.$$

We employ the function $c(x)$ so frequently that it is desirable to introduce a symbol $\bar{x}$ where

$$\bar{x} \equiv c(x) \equiv 1+x$$

and
$$\bar{x}x \equiv x\bar{x} \equiv 0$$
$$x+\bar{x} \equiv 1.$$

Intersection A ∩ B: We have to find a function $m(x, y)$ which take the following values:

$m(x, y) = 1$ when $k \in A \cap B$, i.e., when $k \in A$ and $k \in B$, i.e., when $(x, y) = (1, 1)$.

$m(x, y) = 0$ otherwise, i.e., when $(x, y) = (0, 1)$ or $(1, 0)$ or $(0, 0)$. There is only one function of x and y which vanishes whenever at least one of x and y is zero and not otherwise, namely, $x \times y$, so that we take

$$m(x, y) \overset{\text{def}}{=} xy.$$

From physical considerations we know that the set operation '∩' is commutative and associative, and we require the corresponding function $m(x, y)$ to have the corresponding properties. We see immediately in fact that

$A \cap B \doteq B \cap A$ is represented by $m(x, y) \equiv m(y, x)$

(the operation '×' is commutative) and

$A \cap (B \cap C) \doteq (A \cap B) \cap C$ is represented by

$$m[x, m(y, z)] \equiv m[m(x, y), z], \quad \text{i.e.,} \quad x(yz) \equiv (xy)z$$

and we may write $m(x, y, z)$ for xyz

(the operation '×' is associative).

Union A ∪ B: The 'union function' $u(x, y)$ is required to take the values:

$u(x, y) = 1$ for the pairs $(x, y) = (1, 1), (1, 0), (0, 1)$, and
$u(x, y) = 0$ for $(x, y) = (0, 0)$.

We could use what we already know of set relations to devise a form for $u(x, y)$; e.g.,

$$A \cup B \doteq \widetilde{\tilde{A} \cap \tilde{B}}$$

so that
$$u(x, y) \equiv c[m\{c(x), c(y)\}],$$
$$\equiv c[m(\bar{x}, \bar{y})],$$

but we could also attack the problem directly as a problem in algebra.

Since $x^2 \equiv x$, the most complicated function in two variables that can exist in binary algebra is

$$f(x, y) \equiv a+bx+cy+dxy,$$

where a, b, c, d each takes only the values 1 or 0.

There are therefore only $2^4 = 16$ possible forms of the function (including the two constant forms $a+0x+0y+0xy$) corresponding exactly to the 16 subsets determined by a two-way classification (p. 98); we list these later.

We substitute the various pairs of values of (x, y) into this function, and the corresponding values required to be taken by the function $u(x, y)$ then give equations to determine a, b, c, d.

$$\begin{array}{rrll}
 & & a+bx+cy+dxy & \equiv u(x, y) \\
(x, y) = & (0, 0) & a & = 0 \\
 & (1, 0) & a+b & = 1 \\
 & (0, 1) & a+\;\; c & = 1 \\
 & (1, 1) & a+b\;+c\;+d & = 1.
\end{array}$$

From these equations in turn we find $a = 0$, $b = 1$, $c = 1$, $d = 1$ and the required function is therefore $u(x, y) \overset{\text{def}}{=} x+y+xy$. Thus

$$u(x, y) \equiv 1+(1+x)(1+y) \equiv c[m(\bar{x}, \bar{y})].$$

which is the functional identity corresponding to

$$\mathrm{A} \cup \mathrm{B} \bumpeq \widetilde{\tilde{\mathrm{A}} \cap \tilde{\mathrm{B}}}.$$

$u(x, y)$ is symmetric in x and y corresponding to the commutativity of '$\cup$'. To check the associative property we have to show that

$$u[x, u(y, z)] \equiv u[u(x, y), z].$$

$$\begin{aligned}
u[x, u(y, z)] &\equiv x.\, u(y, z)+x+u(y, z) \\
&\equiv (xyz+xy+xz)+x+(y+z+yz) \\
&\equiv 1+(1+x)(1+y)(1+z) \equiv c[m(\bar{x}, \bar{y}, \bar{z})].
\end{aligned}$$

This is symmetric in x, y, z so that

$$\begin{aligned}
u[x, u(y, z)] &\equiv u[z, u(y, x)] \quad \text{(interchanging } x \text{ and } z\text{)} \\
&\equiv u[u(x, y), z] \quad \text{(since } u(h, k) \text{ is symmetric in } h \text{ and } k\text{)}.
\end{aligned}$$

We look next at the two distribution properties:

The relation $\mathrm{A} \cap (\mathrm{B} \cup \mathrm{C}) \bumpeq (\mathrm{A} \cap \mathrm{B}) \cup (\mathrm{A} \cap \mathrm{C})$ requires that

$$m[x, u(y, z)] \equiv u[m(x, y), m(x, z)].$$

$$\begin{aligned}
m[x, u(y, z)] &\equiv m(x, y+z+yz) \\
&\equiv xy+xz+xyz. \\
u[m(x, y), m(x, z)] &\equiv u(xy, xz) \\
&\equiv xy+xz+xyxz \equiv xy+xz+xyz \\
&\equiv m[x, u(y, z)].
\end{aligned}$$

For the relation $A \cup (B \cap C) \bumpeq (A \cup B) \cap (A \cup C)$ we require

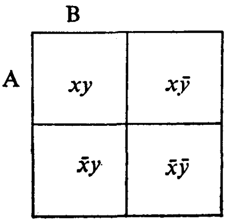
$$\begin{aligned}
u[x, m(y, z)] &\equiv m[u(x, y), u(x, z)].\\
u[x, m(y, z)] &\equiv u(x, yz)\\
&\equiv x+yz+xyz.\\
m[u(x, y), u(x, z)] &\equiv (x+y+xy)(x+z+xz)\\
&\equiv (x+\bar{x}y)(x+z+xz)\\
&\equiv x(\bar{x}z+x)+\bar{x}y(x\bar{z}+z)\\
&\equiv x^2+\bar{x}yz\\
&\equiv x+(1+x)yz\\
&\equiv u[x, m(y, z)].
\end{aligned}$$

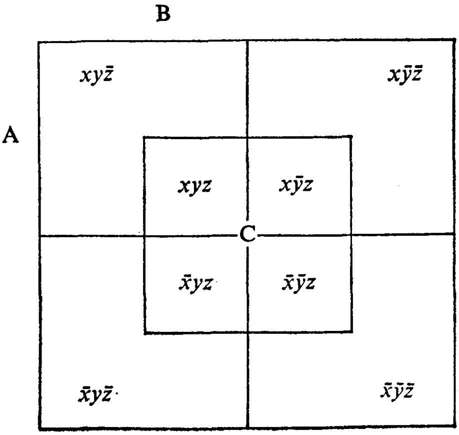
U, Ø are represented respectively by the constant functions 1, 0. Thus the various pairs of corresponding statements involving U and Ø are

1. $A \cap U \bumpeq A$: $m(x, 1) \equiv x \times 1 \equiv x$,
2. $A \cup \varnothing \bumpeq A$: $u(x, 0) \equiv x+0+x \times 0 \equiv x$,
3. $A \cup U \bumpeq U$: $u(x, 1) \equiv x+1+x \times 1 \equiv 1$,
4. $A \cap \varnothing \bumpeq \varnothing$: $m(x, 0) \equiv x \times 0 \equiv 0$,
5. $A \cap \tilde{A} \bumpeq \varnothing$: $m(x, \bar{x}) \equiv x\bar{x} \equiv 0$,
6. $A \cup \tilde{A} \bumpeq U$: $u(x, \bar{x}) \equiv x+\bar{x}+x\bar{x} \equiv 1$.

The model therefore is satisfactory: all the axioms of the set-algebra may be obtained as consequences of the axioms of the binary algebra together with the prescription of the functional forms in the binary algebra which are to correspond to the operations in the set-algebra.

The functions corresponding to the primary subsets are:





For example, $k \in \tilde{\mathrm{A}} \cap \mathrm{B} \cap \tilde{\mathrm{C}}$ if and only if the components of the characteristic sequence of k satisfy $\bar{x}y\bar{z} = 1$, i.e., $y(1+x)(1+z) = 1$. These diagrams follow of course exactly the pattern of the characteristic sequence diagrams (Ch. 6, pp. 92-93).

Exercise 1. Find the characteristic functions of $(\mathrm{A} \cup \mathrm{B}) \cap (\mathrm{C} \cup \mathrm{D})$ and $(\mathrm{A} \cap \mathrm{C}) \cup (\mathrm{A} \cap \mathrm{D}) \cup (\mathrm{B} \cap \mathrm{C}) \cup (\mathrm{B} \cap \mathrm{D})$ and verify that the two subsets are identical.

Exercise 2. The set difference

$$\mathrm{A}-\mathrm{B} \stackrel{\text{def}}{=} \mathrm{A} \cap \tilde{\mathrm{B}}.$$

(i) Find the characteristic function $d(x, y)$ of $\mathrm{A}-\mathrm{B}$, both by direct calculation of the coefficients in the form

$$d(x, y) \equiv kxy+lx+my+n$$

and by considering $m(x, \bar{y})$.

(ii) Prove that

$$\mathrm{A}-(\mathrm{B}-\mathrm{C}) \stackrel{\frown}{=} (\mathrm{A}-\mathrm{B}) \cup (\mathrm{A} \cap \mathrm{C})$$

by identifying the functions $d[x, d(y, z)]$ and $u[d(x, y), m(x, z)]$.

Prove similarly the identities

(iii) $(\mathrm{A}-\mathrm{B})-\mathrm{C} \stackrel{\frown}{=} (\mathrm{A}-\mathrm{B}) \cap (\mathrm{A}-\mathrm{C})$,
(iv) $(\mathrm{A}-\mathrm{B}) \cap \mathrm{C} \stackrel{\frown}{=} (\mathrm{A}-\mathrm{B}) \cap (\mathrm{C}-\mathrm{B})$,
(v) $(\mathrm{A} \cap \mathrm{B})-\mathrm{C} \stackrel{\frown}{=} \mathrm{A} \cap (\mathrm{B}-\mathrm{C})$,
(vi) $(\mathrm{A}-\mathrm{B}) \cup \mathrm{C} \stackrel{\frown}{=} (\mathrm{A} \cup \mathrm{C})-(\mathrm{B}-\mathrm{C})$,
(vii) $\mathrm{A}-(\mathrm{B} \cup \mathrm{C}) \stackrel{\frown}{=} (\mathrm{A}-\mathrm{C})-\mathrm{B}$.

Exercise 3. The operation σ:

$$\mathrm{A} \,\sigma\, \mathrm{B} \stackrel{\text{def}}{=} \tilde{\mathrm{A}} \cup \mathrm{B}.$$

Write $s(x, y)$ for the characteristic function of $\mathrm{A} \,\sigma\, \mathrm{B}$. Prove that

(i) $s(x, y) \equiv \bar{x}+xy \equiv c[d(x, y)]$,
(ii) $\mathrm{A} \,\sigma\, (\mathrm{B} \,\sigma\, \mathrm{C}) \stackrel{\frown}{=} \mathrm{B} \,\sigma\, (\mathrm{A} \,\sigma\, \mathrm{C})$,
(iii) $(\mathrm{A} \,\sigma\, \mathrm{B}) \,\sigma\, \mathrm{C} \stackrel{\frown}{=} (\mathrm{A} \cup \mathrm{C})-(\mathrm{B}-\mathrm{C}) \stackrel{\frown}{=} (\mathrm{A} \cup \mathrm{C}) \cap (\mathrm{B} \,\sigma\, \mathrm{C})$.

Exercise 4. Prove that the characteristic function $j(x, y)$ of $\mathrm{A}+\mathrm{B}$ is

$$j(x, y) \equiv x+y.$$

(i) This verifies immediately that the set operation '+' is commutative and associative, that '$\cap$' is distributive over '+' but not vice versa, and that $\mathrm{A}+\mathrm{A} \stackrel{\frown}{=} \varnothing$.

(ii) Prove that

(a) $(\mathrm{A}+\mathrm{B})+(\mathrm{B}+\mathrm{C}) \stackrel{\frown}{=} \mathrm{A}+\mathrm{C}$,

$$\text{(b)}\quad [(A+B)-C]+[A+(B-C)] \bumpeq A+C,$$
$$\text{(c)}\quad [(B+C)-A]+[(C+A)-B] \bumpeq [(A+B)-C].$$

Exercise 5. We have already seen that the function $u(x, y)$ can be expressed in terms of the functions c and m, and this raises the question whether we need two functions or whether, indeed, all three functions can be expressed in terms of one.

Consider the function

$$n(x, y) \overset{\text{def}}{=} (1+x)(1+y) \equiv \bar{x}\bar{y}.$$

The physical interpretation of $n(x, y)$, since $n(x, y) \equiv 1+u(x, y)$, is membership of the set $\widetilde{A \cup B}$, i.e., of $\tilde{A} \cap \tilde{B}$. It is the characteristic function of the members of the set which satisfy the conditions of belonging neither to A nor to B.

We can derive the functions c and u from n as follows

$$\begin{aligned} c &: \ n(x, x) \equiv \bar{x}^2 \equiv \bar{x} \\ u &: \ u(x, y) \equiv n(x, y)+1 \equiv c\{n(x, y)\} \\ &\qquad\qquad \equiv n[n(x, y), n(x, y)]. \end{aligned}$$

Express $m(x, y)$, $d(x, y)$, $s(x, y)$ in terms of the function n alone.

Exercise 6. The characteristic functions of the sixteen subsets determined by a two-way classification: The characteristic sequence of an element k of U under the classifications p_A, p_B is (x, y), and the characteristic function of a subset F is $f(x, y)$, i.e.

$$k \in F \Leftrightarrow f(x, y) = 1.$$

Complete the following table:

$f(x, y)$	F
0	$\emptyset$
1	U
x	A
$1+x$	
y	
$1+y$	
$x+y$	
$1+x+y$	
xy	$A \cap B$

$1+xy$	
$x+xy$	
$1+x+xy$	
$y+xy$	
$1+y+xy$	
$x+y+xy$	$A \cup B$
$1+x+y+xy$	

7.4 *Binary algebra and set relations*

The relation '$\subseteq$': The OPERATIONS '$\cap$', '$\cup$' by means of which new subsets are defined in terms of known subsets lead to

ALGEBRAIC EQUATIONS, which are satisfied by the pairs of values (x, y) of the characteristic sequences of those members of the set U which satisfy some condition. For example, $u(x, y) = 0$ is satisfied when and only when $k \in \widetilde{A \cup B}$, and to

ALGEBRAIC IDENTITIES, which are satisfied by the characteristic sequences of all members of the set U. For example, corresponding to the set identity,

$$A \cup (B \cap C) \bumpeq (A \cup B) \cap (A \cup C),$$

we have the algebraic identity,

$$u[x, m(y, z)] \equiv m[u(x, y), u(x, z)].$$

Such an algebraic identity is purely formal, in the sense that, when the explicit expressions of the functions are written in their simplest forms, the expressions on the two sides of the identity agree term by term.

These equations and identities apply to 'general' subsets, that is, subsets with no specified relations among themselves. But now suppose that our data about the subsets A, B include the statement

$$A \subseteq B.$$

The elements k of U are such that the set $A \cap \tilde{B}$ is empty, so that no element k has characteristic sequence $(1, 0)$. If our only data are $A \subseteq B$, then there can be elements with any one of the other three characteristic sequences. In consequence, for this set U there is the identical relation

$$xy+x = 0,$$

since $xy+x$ takes the value zero for the three admissible pairs $(1, 1)$, $(0, 1)$ and $(0, 0)$ but not for $(1, 0)$.

Thus the statement 'U is such that the subsets A and B are related by $\mathrm{A} \subseteq \mathrm{B}$', is equivalent to the statement 'U is such that

$$xy+x = 0$$

for the components of the characteristic sequences of all members of U'. We may say then:
the RELATION

$$\mathrm{A} \subseteq \mathrm{B}$$

is represented by
the ALGEBRAIC IDENTITY

$$xy+x = 0$$

which may be written as

$$xy = x,$$

or

$$m(x, y) = x,$$

or

$$x\bar{y} = 0,$$

or

$$m(x, \bar{y}) = 0.$$

The relation $\Rightarrow$ which forms the basis for valid argument and the logician's operation $\rightarrow$ which creates a new statement out of two given statements can be explained now in algebraic terms.

The relation $p_A \Rightarrow p_B$ corresponds to the algebraic identity $xy+y+1 = 1$ (i.e., $\bar{x}y = 0$) which corresponds to a restriction of the possible values of the components of the characteristic sequence (x, y). The theorem:

$$(p_A \Rightarrow p_B \quad \text{and} \quad p_B \Rightarrow p_C) \Rightarrow (p_A \Rightarrow p_C)$$

is represented by the theorem

$$(xy+y = 0 \quad \text{and} \quad yz+z = 0) \Rightarrow (xz+z = 0)$$

which can be proved thus:

$$xz+z = x(yz)+z = (xy)z+z = yz+z = 0.$$

The operation $p_A \rightarrow p_B$ corresponds to the algebraic function $xy+y+1$ which takes the value 1 for the characteristic sequence (x, y) corresponding to any element k of the subset

$$\{k\colon k \text{ satisfies } p_A \rightarrow p_B\},$$

and 0 for any element of the complementary subset. The theorem

$$[(p_A \rightarrow p_B \wedge p_B \rightarrow p_C)] \Rightarrow (p_A \rightarrow p_C)$$

corresponds to the set relation

$$[(\mathrm{A}\ \sigma\ \mathrm{B}) \cap (\mathrm{B}\ \sigma\ \mathrm{C})] \subseteq (\mathrm{A}\ \sigma\ \mathrm{C}),$$

and hence to the formal algebraic identity

$$[(xy+y+1)(yz+z+1)][(xz+z+1)+1] \equiv 0,$$

i.e.,

$$(xy+\bar{y})(yz+\bar{z})\bar{x}z \equiv 0,$$

which is easily verified.

Identities corresponding to other relations are considered in the following exercises.

Exercise 7. Specially related subsets: We have just seen that if the characteristic sequence of any member of U corresponding to a dissection of U by two subsets A, B is (x, y), then a necessary and sufficient condition for A $\subseteq$ B is that the components of the characteristic sequence of every member of U satisfy the condition $xy+x = 0$. In this exercise we construct the table of the 14 non-constant functions listed in Exercise 5, but the condition now is

$$f(x, y) = 0,$$

and represents a relation among A, B and U. $f(x, y) = 0$ may be regarded as specifying that a certain region on the Venn diagram corresponds to the empty set. In the table, list the functions $f(x, y)$, the corresponding empty set, and, where significant, an alternative expression of the relation among A, B, U.

$f(x, y) = 0$	$\mathrm{F} \bumpeq \emptyset$	
x	$\mathrm{A} \bumpeq \emptyset$	$\tilde{\mathrm{A}} \bumpeq \mathrm{U}$
$1+x$	$\tilde{\mathrm{A}} \bumpeq \emptyset$	$\mathrm{A} \bumpeq \mathrm{U}$
y		
$1+y$		
$x+y$		
$1+x+y$		
xy	$\mathrm{A} \cap \mathrm{B} \bumpeq \emptyset$	$\mathrm{A} \subseteq \tilde{\mathrm{B}}, \mathrm{B} \subseteq \tilde{\mathrm{A}}$
$1+xy$		
$x+xy$		
$1+x+xy$		
$y+xy$		
$1+y+xy$		
$x+y+xy$	$\mathrm{A} \cup \mathrm{B} \bumpeq \emptyset$	$\tilde{\mathrm{A}} \bumpeq \tilde{\mathrm{B}} \bumpeq \mathrm{U}$
$1+x+y+xy$		

7.5 *Characteristic functions*

Now suppose there are *n* classifications so that the relations of each element of the set to the classifications can be represented by a sequence $(x_1\ x_2, \ldots, x_n)$ of 0's and 1's. There are therefore altogether 2^n 'primary' subsets, including Ø, corresponding to the 2^n possible selections of 0's and 1's in the sequence and, as we saw in the last chapter, altogether 2^{2^n} possible subsets. Each of these subsets will be represented by a specific function of $x_1, \ldots, x_n$ which takes the value 1 or 0 according as a member of U does or does not belong. There are in fact (including 0 and 1 as functions) altogether 2^{2^n} possible functions of the *n* variables in binary algebra.
We may write them as

$$\alpha + \Sigma\alpha_i x_i + \Sigma\alpha_{ij} x_i x_j + \Sigma\alpha_{ijk} x_i x_j x_k + \ldots + \Sigma\alpha_{i_1 \ldots i_r} x_{i_1} x_{i_2} \ldots x_{i_r}$$
$$+ \ldots + \alpha_{12 \ldots n} x_1 x_2 x_3 \ldots x_n$$

where $\Sigma\alpha_{i_1 \ldots i_r} x_{i_1} \ldots x_{i_r}$ is the sum of the products *r* at a time of the *n* variables x_i, each multiplied by a coefficient $\alpha_{i_1 \ldots i_r}$ (which may be 0 or 1).

Such a function $f(x_1, x_2, \ldots, x_n)$ ($\equiv f(x)$ say) is called the characteristic function of the subset F. Its property is this: if (x) is the characteristic sequence of a member *k* of U relative to subsets $A_1, \ldots, A_n$ then

$$f(x) = 1 \Leftrightarrow k \in \mathrm{F}$$
$$f(x) = 0 \Leftrightarrow k \in \tilde{\mathrm{F}}.$$

We have of course

$$c[f(x)] \equiv 1 + f(x)$$
$$m[f(x), g(x)] \equiv f(x).g(x)$$
$$u[f(x), g(x)] \equiv f(x) + g(x) + f(x).g(x).$$

Now suppose that four chosen subsets F, G, H, K, are such that

$$\mathrm{F} \cap \mathrm{G} \simeq \mathrm{H} \cap \mathrm{K} \simeq \mathrm{T}.$$

Then among the corresponding characteristic functions we have the identical relations

$$f(x).g(x) \equiv h(x).\, k(x) \equiv t(x),$$

i.e., $t(x)$ has two different pairs of factors, which need not be equivalent in the sense that they can all be broken up into other factors which over-all are the same for both *fg* and *hk*.

As a simple example consider the identity corresponding to

$$(\mathrm{A} \cup \mathrm{B}) \cap (\widetilde{\mathrm{A} \cap \mathrm{B}}) \bumpeq (\mathrm{A} \cap \tilde{\mathrm{B}}) \cup (\tilde{\mathrm{A}} \cap \mathrm{B}),$$

namely,

$$\begin{aligned} m\{u(x, y), c[m(x, y)]\} &\equiv u[m(x, \bar{y}), m(\bar{x}, y)] \\ (x+y+xy)(1+xy) &\equiv x\bar{y}+\bar{x}y+x\bar{y}\bar{x}y \\ &\equiv x(1+y)+y(1+x) \end{aligned}$$

i.e.,

$$(x+y+xy)(1+xy) \equiv x+y.$$

The function $x+y$ is 'irreducible' in the ordinary meaning of the term, but it is nevertheless the product of two quadratic factors in the system of algebra under discussion.

In fact, in contrast to ordinary algebra, there is in this binary algebra no simple 'unique factorisation theorem'.

The reason for this is not hard to find: a relation, '$ax^2+bx+c = 0$ for all x' in ordinary algebra is valid only for $a = 0$, $b = 0$, $c = 0$. But in binary algebra where 'for all x' can be interpreted only as 'for $x = 1$ and $x = 0$',

$$ax^2+bx+c = 0$$

implies only

$$\begin{cases} a+b+c = 0 & (x = 1) \\ c = 0 & (x = 0) \end{cases}$$

i.e., *either* $a = b = c = 0$, *or* $a = b = 1$, $c = 0$; it is the existence of the non-trivial identity

$$x\bar{x} \equiv x^2+x \equiv 0$$

which destroys unique factorisability. The identity

$$(x+y+xy)(1+xy) \equiv x+y$$

found above, can be written as

$$(x+y)+xy(1+x+y+xy) \equiv x+y$$

i.e.,

$$(x+y)+xy\bar{x}\bar{y} \equiv x+y.$$

Exercise 8. (i) Mark on the 2^3 Venn diagram the region for which the characteristic function is $x+y+z+xyz$.

(ii) The subsets A, B, C are such that the characteristic sequence of every element of U satisfies the identical relation $x+y+z+xyz \equiv 0$. Prove that U is the union of five disjoint subsets P, Q, R, S, T such that

$$\begin{aligned} \mathrm{A} &\bumpeq \mathrm{P} \cup \mathrm{Q} \cup \mathrm{R} \\ \mathrm{B} &\bumpeq \mathrm{P} \cup \mathrm{Q} \cup \mathrm{S} \\ \mathrm{C} &\bumpeq \mathrm{P} \cup \mathrm{R} \cup \mathrm{S}. \end{aligned}$$

7.6 *Another algebraic model: rational characteristic functions*

The algebraic system to be constructed now is closely similar to the binary algebra that we have so far used; the variables are the components of the characteristic sequences, but the algebra is 'ordinary' algebra with the usual rules for addition, subtraction and multiplication, but with these restrictions: the domain of the variables is {0, 1}, and for this domain of the variables the range of any function used is {0, 1}. The coefficients can assume any integer value consistent with the above conditions. The problems to be solved are precisely the same as before, and the methods of solution the same.

We shall designate these functions RATIONAL CHARACTERISTIC FUNCTIONS and those introduced in §7.5, in which variables and coefficients both belong to the field of remainders modulo 2, BINARY CHARACTERISTIC FUNCTIONS.

When the domain of x is {0, 1}, we have the identical relations

$$x \equiv x^2 \equiv x^3 \equiv \dots$$

and consequently, for this domain, any function

$$a+bx+cx^2+dx^3+ex^4+ \dots$$

takes the same values as

$$a+(b+c+d+e+ \dots)x.$$

In this system we consider therefore only functions of the forms

$$a+bx,\ a+bx+cy+dxy, \dots,$$

and in any manipulation we replace x^2, x^3, ... by x.

Exercise 9. (i) Prove that the rational characteristic functions of $\tilde{\mathrm{A}}$, $\mathrm{A} \cap \mathrm{B}$, $\mathrm{A} \cup \mathrm{B}$ are

$$\begin{aligned} c(x) &\equiv 1-x \quad (\equiv \bar{x}) \\ m(x,y) &\equiv xy \\ u(x,y) &\equiv x+y-xy \equiv c[m(\bar{x},\bar{y})]. \end{aligned}$$

(ii) Find the characteristic functions, $d(x,y)$, $s(x,y)$, $n(x,y)$, of $\mathrm{A}-\mathrm{B}$, $\mathrm{A}\ \sigma\ \mathrm{B}$, $\tilde{\mathrm{A}} \cap \tilde{\mathrm{B}}$.

(iii) List all functions $a+bx+cy+dxy$ of which the range is 0 and 1 when the domain of the variables is 0 and 1. [Follow the consequences of taking (x,y) to be in turn $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$.]

(iv) Find a function $f(x,y,z)$, having range 0 and 1 when the domain of the variables is 0 and 1, which includes at least one term with a coefficient numerically greater than 2. Mark the corresponding region on the Venn diagram [e.g., Exercise 8 (i)].

(v) Verify that

$$s(x, y)\, s(y, z)\, c[s(x, z)] \equiv 0,$$

i.e., in general terms, that when the domain of the variables is suitably restricted, it is possible to find a product of functions which vanishes identically without any one of the functions being identically zero.

(vi) Prove that the rational characteristic functions of A+B, A+B+C, $\sum_{1}^{r} \mathrm{A}_i$ are

$$\begin{aligned} j(x, y) &\equiv x+y-2xy \\ j(x, y, z) &\equiv x+y+z-2(xy+xz+yz)+4xyz \\ j(x_1, \ldots, x_r) &\equiv \Sigma x_i - 2\Sigma x_i x_j + 4\Sigma x_i x_j x_k - \ldots \\ &\quad + (-2)^{s-1}\, \Sigma x_{i_0} x_{i_1} \ldots x_{i_s} + \ldots + (-2)^{r-1}\, x_1 x_2 \ldots x_r. \end{aligned}$$

The 2^{2^n} subsets defined by n classifications are all expressible in terms of the operations of complementation, union and intersection on the subsets $\mathrm{A}_1, \ldots, \mathrm{A}_n$. That is to say, any subset H is obtained from the subsets F, G, either as $\tilde{\mathrm{F}}$ or $\mathrm{F} \cap \mathrm{G}$ or $\mathrm{F} \cup \mathrm{G}$, F and G themselves having been obtained in the same way from other pairs of subsets, and so on down to ultimate pairs A_i, A_j. Write

$$h(x)\ (=h(x_1, \ldots, x_n)), \quad f(x),\ g(x)$$

for the characteristic functions of H, F, G, then

$$h(x) \equiv c[f(x)] \quad \text{or} \quad m[f(x), g(x)] \quad \text{or} \quad u[f(x), g(x)].$$

So that if the ranges of $f(x)$, $g(x)$ are both 0 and 1, so also is the range of $h(x)$. It follows therefore, by algebraic induction, that the range of $h(x)$ is 0 and 1, as it must be if the system we have devised is to provide a model for relations among and operations on subsets.

Exercise 10. (i) Prove by induction on r, that if

$$\begin{aligned} h(x_1, \ldots, x_r) \equiv \alpha + \Sigma\alpha_i x_i + \Sigma\alpha_{ij} x_i x_j + \ldots + \Sigma\alpha_{i_1 \ldots i_s} x_{i_1} \ldots x_{i_s} \\ + \ldots + \alpha_{1 \ldots r} x_1 \ldots x_r, \end{aligned}$$

where $\Sigma\alpha_{i_1 \ldots i_s} x_{i_1} \ldots x_{i_s}$ is a sum over all products of s different terms from the set $\{x_1, \ldots, x_r\}$, is such that $h(x_1, \ldots, x_r) = 0$ for every set of values $\{x_i\}$, $x_i = 0, 1$, then all the coefficients $\alpha_{i_1 \ldots i_s}$ are zero.

(ii) Prove that, given any subset F in the dissection of U by the r subsets $A_1, \ldots, A_r$, a unique characteristic function $f(x_1, \ldots, x_r)$ can be found which takes the value 1 for elements of F and 0 for elements of $\widetilde{F}$.

(iii) Prove that every function $f(x_1, \ldots, x_r)$ of the form in (i) which has range $\{0, 1\}$ when the variables have domain $\{0, 1\}$ can be obtained by a succession of operations of forming the function $n[f(\boldsymbol{x}), g(\boldsymbol{x})]$ starting with the basic functions

$$n(x_i, x_j) \equiv x_i x_j - x_i - x_j + 1.$$

7.7 *The synthesis and analysis of characteristic functions*

Any subset is compounded of primary subsets, so that from one point of view we may regard a 'given subset' as having been prescribed by a list of its component primary subsets under a given dissection by n subsets. When the subset is given in this way we can construct the characteristic function directly. Thus suppose that a subset

$$F \bumpeq \{H^{(1)}, H^{(2)}, \ldots, H^{(r)}\}^{*}$$

where $H^{(i)}$ are primary subsets. Each primary subset H will have been defined as $H \bumpeq G_1 \cap G_2 \cap \ldots \cap G_n$ where each G_j is defined as one of the two complementary sets A_j or $\tilde{A}_j$.

The characteristic function $h(\boldsymbol{x})$ of the primary subset H is

$$h(\boldsymbol{x}) = t_1 t_2 \ldots t_n$$

where $t_k = x_k$ if $G_k \bumpeq A_k$,

and $t_k = \tilde{x}_k$ if $G_k \bumpeq \tilde{A}_k$.

If $h^{(i)}$ is the characteristic function of $H^{(i)}$ then, since $H^{(i)} \cap H^{(j)} \bumpeq \emptyset$ (the subsets being primary subsets)

$$u(h^{(i)}, h^{(j)}) \equiv h^{(i)} + h^{(j)} - 0.$$

Thus if

$$F \bumpeq \{H^{(1)}, H^{(2)}, \ldots, H^{(r)}\},$$

*Cf. footnote to p. 92.

Since $H^{(i)}$, being primary subsets, are mutually non-intersecting, we could write F equally well as

$$\begin{aligned} F &\bumpeq H^{(1)} \cup H^{(2)} \cup \ldots \cup H^{(r)} \\ &\bumpeq \mathrm{U}(H^{(i)}),\ i = 1, \ldots, r \end{aligned}$$

or as

$$\begin{aligned} F &\bumpeq H^{(1)} + H^{(2)} + \ldots + H^{(r)} \\ &\bumpeq \Sigma H^{(i)},\ i = 1, \ldots, r. \end{aligned}$$

the corresponding characteristic function $f(\mathbf{x})$ is given by

$$f(\mathbf{x}) \equiv h^{(1)}(\mathbf{x})+h^{(2)}(\mathbf{x})+\ldots+h^{(r)}(\mathbf{x}).$$

This identity is valid whether we use binary characteristic functions or rational characteristic functions.

If we are given the index number of a subset as described in §6.4, we are effectively given the constituent primary subsets. As an example, suppose the given subset F (in a three-way classification) has index number 234.

$$234 = 0+2+0+8+0+32+64+128,$$

so that

$$\begin{aligned} \mathrm{F} &\doteqdot \{[1], [3], [5], [6], [7]\}. \\ &\doteqdot \{(1,0,0), (1,1,0), (1,0,1), (0,1,1), (1,1,1)\} \\ &\doteqdot (\mathrm{A}\cap\tilde{\mathrm{B}}\cap\tilde{\mathrm{C}})+(\mathrm{A}\cap\mathrm{B}\cap\tilde{\mathrm{C}})+(\mathrm{A}\cap\tilde{\mathrm{B}}\cap\mathrm{C}) \\ &\qquad +(\tilde{\mathrm{A}}\cap\mathrm{B}\cap\mathrm{C})+(\mathrm{A}\cap\mathrm{B}\cap\mathrm{C}). \end{aligned}$$

It follows that the rational characteristic function is

$$\begin{aligned} f(x,y,z) &= x\bar{y}\bar{z}+xy\bar{z}+x\bar{y}z+\bar{x}yz+xyz \\ &= x(1-y)(1-z)+xy(1-z)+xz(1-y)+yz(1-x) \\ &\qquad +xyz \\ &= x+yz-xyz. \end{aligned}$$

Thus the synthesis of a subset from primary subsets can be matched by a synthesis of the characteristic function as the sum of simple products $t_1t_2\ldots t_n$ where each t_i is either x_i or $\bar{x}_i$.

Now suppose we are given a characteristic function, and are required to determine the subset to which it corresponds. It would clearly be very laborious to discover directly, for example, how $x+yz-xyz$ could be expressed as a sum of simple products $t_1t_2t_3$. Instead we have to locate the characteristic sequences of these primary subsets by discovering for which characteristic sequences the function takes the value 1.

Take again

$$f(x,y,z) = x+yz-xyz,$$

and construct the table of values, thus:

(x,y,z):	000	100	010	110	001	101	011	111
$f(x,y,z)$:	0	1	0	1	0	1	1	1 .

This determines $f(x,y,z)$ as

$$f(x,y,z) = x\bar{y}\bar{z}+xy\bar{z}+x\bar{y}z+\bar{x}yz+xyz$$

and F as {[1], [3], [5], [6], [7]}.

Exercise 11. Find the rational characteristic function $f(x,y,z,w)$ of the subset F of which the index number in a four-way classification is 2345 and verify your answer by determining directly the characteristic sequences of the primary subsets of which the subset is compounded.

For readers acquainted with simple matrix algebra another aspect of this synthesis and analysis is discussed in the appendix to this chapter (p. 122).

7.8 *Boolean algebra*

The difference between the earlier approach to set-algebra which led to the Boolean system, and the approach in this chapter through the characteristic sequences, is that the earlier approach was concerned with the subsets A, B, C, . . ., their complements, intersections and unions, while the characteristic sequences are concerned with the individual members of the set, and labelling them systematically, in such a way that the subsets A, B, C, . . . and the derived subsets are synthesised as sets of characteristic sequences (labels) which satisfy appropriate algebraic conditions. Our task now is to discover if a more direct connection could be established between the binary algebra and the Boolean algebra.

What in fact we do is to invent three new operations on the elements of a characteristic sequence to replace the characteristic functions of the elements considered as the marks '0' and '1' in binary algebra.

Let us then set down the actual tables of values of the characteristics, using $\bar{x}$, $x \times y$ and $x * y$ to represent the operations of complementation, intersection and union.

$\bar{A} : \bar{x}$

x	1	0
$\bar{x}$	0	1

$A \cap B : x \times y$

$x \backslash y$	1	0
1	1	0
0	0	0

('×' is in fact the '×' of ordinary arithmetic)

A∪B : $x * y$

$x \backslash y$	1	0
1	1	1
0	1	0

As we did with the binary algebra, let us assume that these tables provide the axioms of the system, and investigate how far the relations among the corresponding set operations can be deduced from them. We show in fact that all the properties of commutation (which is obvious), association and distribution follow from them.

The duality of this system is immediately apparent, for

$x \times y = 0$ if and only if at least one of x and y is 0
$x * y = 1$ if and only if at least one of x and y is 1.

From the complementation table we see that the table for

$\bar{x} * \bar{y}$ is

$\bar{x} \backslash \bar{y}$	1	0
1	0	1
0	1	1

so that $\bar{x} * \bar{y} = \overline{x \times y}$.

To prove '$*$' is associative.*

$$\begin{aligned}(\bar{x} * \bar{y}) * \bar{z} &= \overline{x \times y} * \bar{z} = \overline{(x \times y) \times z} = \overline{x \times y \times z} \\ &= \overline{(y \times z) \times x} = \overline{y \times z} * \bar{x} = (\bar{y} * \bar{z}) * \bar{x} = \bar{x} * (\bar{y} * \bar{z}).\end{aligned}$$

Exercise 12. (i) Prove similarly that '$*$' is distributive over '×'.

(ii) Show that the operation '$\downarrow$' defined by the table

$x \downarrow y$

$x \backslash y$	1	0
1	0	0
0	0	1

is commutative but not associative, and that the operations '—', '×' and '$*$' can all be expressed in terms of '$\downarrow$'.

It follows that Boolean algebra can be based on:

Axioms: the single table for '$\downarrow$'.

---

*The proof can be written more compactly if we take $\bar{x}$ etc. as 'pronumerals', rather than x etc.

Definitions: '−', '×', '∗' in terms of '↓'.

In standard texts on Boolean algebra it is customary to write:

xy for $x \times y$ and

$x+y$ for $x * y$.

In the present context we have used the different symbols to avoid confusion of meaning.

With practice this form of Boolean algebra is at least as easy to handle as ordinary algebra. For example, to prove

$$\mathrm{A} \cap (\mathrm{B}-\mathrm{C}) \leftrightharpoons (\mathrm{A}-\mathrm{C}) \cap (\mathrm{B}-\mathrm{C})$$

we have to prove

$$x(y\bar{z}) \equiv (x\bar{z})(y\bar{z}).$$

Using the associative and commutative properties we have

$$(x\bar{z})(y\bar{z}) \equiv xy\bar{z}\bar{z} \equiv xy\bar{z}.$$

Exercise 13. Exercises 7, 9, 10 in Chapter 4.

APPENDIX TO CHAPTER 7

7.9 *An application of matrix algebra*

For the reader who has some acquaintance with matrix algebra a simple algebraic relation between the synthesis and analysis of a characteristic function can be devised. Let us confine the discussion initially to a dissection by two subsets; we have essentially two vectors associated with each subset F:

the index sequence (§6.4) which we will now call the 'index-vector'

$$\mathbf{w} = \begin{bmatrix} w_0 \\ w_1 \\ w_2 \\ w_3 \end{bmatrix},$$

depending on the constituent primary subsets of F and determined by

$$w_i = \begin{cases} 1 \text{ if } [i] \subseteq \mathrm{F} \\ 0 \text{ if } [i] \cap \mathrm{F} \bumpeq \varnothing, \end{cases}$$

and the 'coefficient-vector'

$$\mathbf{a} = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

determined by the characteristic function,

$$f(x, y) \equiv a+bx+cy+dxy,$$

of F with the terms written in a certain order. We shall assume that $f(x, y)$ is the rational characteristic function—it can be immediately reduced to binary form by replacing a, b, c, d by their remainders modulo 2.

w and **a** are connected by the equations

$$\begin{aligned} w_0 &= f(0, 0) = a \\ w_1 &= f(1, 0) = a+b \\ w_2 &= f(0, 1) = a+c \\ w_3 &= f(1, 1) = a+b+c+d, \end{aligned}$$

which may be written as

$$\mathbf{w} = \mathbf{M}_2\mathbf{a}$$

where

$$\mathbf{M}_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

(The subscript 2 refers to the dissection by 2 subsets.)

It can be verified immediately that $\mathbf{M}_2$ is non-singular and that

$$\mathbf{M}_2^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

so that

$$\mathbf{a} = \mathbf{M}_2^{-1}\mathbf{w}.$$

Thus, given the constituent primary subsets of F, that is, given **w**, the operation of synthesising the characteristic equation is represented by $\mathbf{a} = \mathbf{M}_2^{-1}\mathbf{w}$, the characteristic function $f(x, y)$ being

$$[a, b, c, d] \begin{bmatrix} 1 \\ x \\ y \\ xy \end{bmatrix},$$

which we could write as $f(x, y) \equiv \mathbf{a}^T \xi_2$.

Conversely, given the characteristic function $\mathbf{a}^T \xi_2$, the operation of analysing F into its constituent primary subsets is represented by

$$\mathbf{w} = \mathbf{M}_2\mathbf{a}.$$

In taking the step from two to three classifications we have to select carefully the order in which we write the terms of the characteristic function, so as to preserve the greatest measure of symmetry. In fact, the 'natural' order proves to be the best, namely, that exhibited in the following table:

Index number of primary subset	Char. sequence of primary subset	Term in char. function of a subset
[0]	(0, 0, 0)	1
[1]	(1, 0, 0)	x
[2]	(0, 1, 0)	y
[3]	(1, 1, 0)	xy
[4]	(0, 0, 1)	z
[5]	(1, 0, 1)	xz
[6]	(0, 1, 1)	yz
[7]	(1, 1, 1)	xyz

That is, we build up the characteristic function in the following pattern:

$$a+bx+y(c+dx)+z[e+fx+y(g+hx)].$$

When the components of the coefficient-vector $\mathbf{a}$ are written in this order, the relation connecting it with the index-vector $\mathbf{w}$ is

$$\begin{bmatrix} w_0 \\ w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \\ w_7 \end{bmatrix} = \begin{array}{c} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \\ \begin{array}{cccccccc} 000 & 100 & 010 & 110 & 001 & 101 & 011 & 111 \end{array} \end{array} \begin{array}{cc} \begin{bmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \end{bmatrix} & \begin{array}{c} 000 \\ 100 \\ 010 \\ 110 \\ 001 \\ 101 \\ 011 \\ 111 \end{array} \end{array}$$

say,

$$\mathbf{w} = \mathbf{M}_3\mathbf{a}.$$

The pattern of the matrix $\mathbf{M}_n$ for the dissection by n subsets is now clear. If we write

$$\mathbf{M}_0 = 1 \text{ (a matrix of a single row and column)}$$

and

$$\mathbf{M}_1 = \begin{bmatrix} \mathbf{M}_0 & 0 \\ \mathbf{M}_0 & \mathbf{M}_0 \end{bmatrix}, \text{ i.e., } \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

then

$$\mathbf{M}_2 = \begin{bmatrix} \mathbf{M}_1 & 0 \\ \mathbf{M}_1 & \mathbf{M}_1 \end{bmatrix}$$

and

$$\mathbf{M}_3 = \begin{bmatrix} \mathbf{M}_2 & 0 \\ \mathbf{M}_2 & \mathbf{M}_2 \end{bmatrix}.$$

Moreover, from the rules for multiplying partitioned matrices:

$$\mathbf{M}_1^{-1} = \begin{bmatrix} \mathbf{M}_0^{-1} & 0 \\ -\mathbf{M}_0^{-1} & \mathbf{M}_0^{-1} \end{bmatrix}, \text{ i.e., } \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$$

$$\mathbf{M}_2^{-1} = \begin{bmatrix} \mathbf{M}_1^{-1} & 0 \\ -\mathbf{M}_1^{-1} & \mathbf{M}_1^{-1} \end{bmatrix}$$

$$\mathbf{M}_3^{-1} = \begin{bmatrix} \mathbf{M}_2^{-1} & 0 \\ -\mathbf{M}_2^{-1} & \mathbf{M}_2^{-1} \end{bmatrix}.$$

The coefficient-vector $\mathbf{a}$ of the characteristic function $f(x, y, z)$ of a subset F is determined from the index-vector $\mathbf{w}$ of F by

$$\mathbf{a} = \mathbf{M}_3^{-1}\mathbf{w}.$$

The patterns of the matrices $\mathbf{M}_n$, $\mathbf{M}_n^{-1}$ of 2^n rows and columns, for a dissection by n subsets can now be predicted: they are defined inductively by

$$\mathbf{M}_n = \begin{bmatrix} \mathbf{M}_{n-1} & 0 \\ \mathbf{M}_{n-1} & \mathbf{M}_{n-1} \end{bmatrix} \text{ and } \mathbf{M}_n^{-1} = \begin{bmatrix} \mathbf{M}_{n-1}^{-1} & 0 \\ -\mathbf{M}_{n-1}^{-1} & \mathbf{M}_{n-1}^{-1} \end{bmatrix}$$

Exercise 14. The rows and columns of $\mathbf{M}_3$ are numbered 000, 100, 010, 110, ..., 111 in the reversed binary scale. Verify that

(i) The element of $\mathbf{M}_3$ in the row numbered rst and the column numbered $r's't'$ is

$$1 \begin{cases} \text{if } r'\,s'\,t' = 000 \text{ and} \\ \text{if } r = 1 \text{ when } r' = 1, s = 1 \text{ when } s' = 1 \text{ and } t = 1 \text{ when } t' = 1 \end{cases}$$

0 if one at least of r, s, t is 0 when the corresponding digit of $r's't'$ is 1.

(ii) If m and m' are the elements respectively of $\mathbf{M}_3$ and $\mathbf{M}_3^{-1}$ in the column numbered rst and the row numbered $r's't'$, then

$$m' = (-1)^u m$$

where $$u = r+s+t+r'+s'+t'.$$

Chapter 8

ALLOWING FOR UNCERTAINTY AND IGNORANCE

In this chapter we link together two rather dissimilar topics, neither of which is strictly relevant to the development of the subject, though both throw light on the processes by which a subject grows. Up to the present, we have assumed that we are discussing mathematical models of a physical system in which our data are always of the type: this object has property *p*, this other object does not have property *p*. Here we are going to discuss models for systems in which:

I. For each object we are given only the probabilities that it has certain properties.

II. For some objects of a set we have no information in relation to some properties.

8.1 *The process of 'generalisation'*

One of the ways in which Mathematics grows is by 'generalisation'. A striking illustration is provided by the early development of co-ordinate geometry. Descartes set out in about 1617 to invent what would now be described as an 'algebraic model' for Euclidean Geometry, and apply it to proving all the theorems of Euclidean Geometry, particularly those which relate to circles, parabolas, ellipses and hyperbolas (about which Greek mathematicians had discovered and proved far more properties than most present-day mathematicians are aware of). He invented the method of using co-ordinates, and in fact denoted by x and y, as we still do, the distances from his two perpendicular axes.

He published his work in 1637, and gradually the work came to be accepted for what it was, a new, more satisfying and basically simpler way of proving known theorems in Euclidean Geometry. Newton, early in that extraordinarily productive period of his, beginning in 1664, when he devised his theory of gravitation, his method of fluxions (the differential calculus) and the general binomial theorem, also wrote a monograph which set forth the first 'generalisation' of Descartes' work. Descartes had found that all the curves that he had had to consider (they are in fact the plane sections of a right circular cone) were represented in his system of co-ordinates by equations of degree two. Newton saw this as an unnecessary restriction on the use of the method, and in his monograph classified and drew the graphs of all possible types of curves which are represented by equations of degree three—the first new growth on the sapling Descartes had planted, a tree which was to grow and flourish abundantly in the nineteenth century, and bear the seeds of the modern study of topology and algebraic geometry.

We could trace in the same way the growth of the much humbler plant which is the subject of this book. Again its origin lies with the Greeks as 'Logic'. The renaissance of logic (or its conversion to a branch of mathematics), came with the invention of mathematical models of logical operations which we discussed in Chapter 3, the core of which is Boolean algebra. But Boolean algebra, while it can itself form the basis of generalisation, is not the algebra which belongs to or grows out of the ordinary number system, and the broad sweep of generalisation which this would allow (as from Descartes to Newton) is therefore not possible.

In the previous chapter we discussed an 'algebraic model' for Boolean algebra which does use the processes of ordinary arithmetic (the 'field axioms'). The basis of this model is the characteristic sequence of 0's and 1's and functions of the components of the sequence whose range is 0 and 1. A clear direction for mathematical generalisation would be to replace the domain and range, $\{0, 1\}$, by some larger set of numbers, but one would have to do so with some indication of the properties that one ought to require the functions to possess.

In all the work so far we have assumed that we know for certain for every member k of U and for every subset A either that $k \in \mathrm{A}$ or $k \in \tilde{\mathrm{A}}$. We want to investigate now whether we can build a satisfactory system to represent circumstances when our information is less complete. There are two possible ways in which the information may lack completeness, which, using again the children in the class as an example, can be explained as follows:

I. We are not concerned with the individual children, but know merely the number, 24, of children in the class, and the number, 7, who are left-handed. That is, for this class, the only available information about left-handedness is that the 'probability' that any one (unspecified) child is left-handed is 7/24.

II. We know that *A*, *B*, *F*, *J*, *M*, *V* are left-handed and that *C*, *D*, *E*, *K*, *L*, *P*, *Q*, *S*, *T*, *Y* are not left-handed, but have been given no information at all (for some reason the entries on their identifying labels were omitted) about the other children in the class.

I. ALLOWING FOR UNCERTAINTY

8.2 *Numerical data for sets*

As a typical real-life system of the type we are to consider let us take the card-index which lists for each child in a group of parallel classes the subjects he is taking, this information being tabulated in the form:

	English	French	German	Latin	Mathematics	Physics	...
Anne	1	1	0	1	1	0	...
Bill	1	0	1	0	1	1	...
...							

The order of the subjects having been fixed, it is necessary only to enter the characteristic sequence on the card, as, for example: *Anne* (1, 1, 0, 1, 1, 0, . . .).

We assume that each card is filled in completely and correctly; we are going to use the cards to count various subsets of the set of children and to investigate the significance of some of the results obtained.

To make the explanations simpler, we are going to assume that we have 100 cards, that p_A is the statement that 'The child's card records that he is taking subject A', and $p_{\bar{A}}$ that he is not taking subject A; that the subjects we are concerned with are A, B, C, . . ., and that we use A also to designate the subset of the set of 100 cards on which is recorded 'This child is taking subject A', and B, C, . . ., similarly.

Let us confine our attention to three subjects, A, B, C; suppose that the numbers of cards in the variously constituted subsets are:

U	A	B	C
100	75	50	30 .

We need to know also the numbers of cards corresponding to children studying various combinations of subjects. In fact, since there are eight primary subsets determined by a three-way classification, and there could be any number of cards listed in any one of these (provided, in this case of course, that the total of all eight lists is 100), we have to have (including the number of members of U) eight pieces of information, no one of which could be deduced from the others.

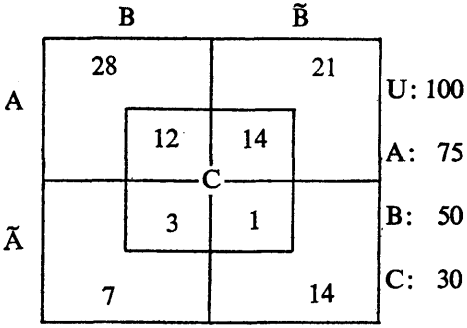
The simplest way to set this information out is by writing the numbers in the regions representing the primary subsets on the Venn diagram, where, in this case again, the totals in the whole region and in the regions representing A, B and C have to be 100, 75, 50, 30 respectively. In terms of our earlier descriptions we could say: 'There are 75 names on list A', etc.

Suppose then the numbers are:

A and B only

	B	$\tilde{B}$
A	40	35
$\tilde{A}$	10	15

A, B and C



Now write

P(A) to mean (at first) the proportion of the whole set of 100 cards, that is, in this case, the percentage of the cards which belong to set A, and

P(A ∩ B) etc., to mean the proportion belonging to (A ∩ B) etc. So that, from the diagram,

$$P(A) = 75\%, \qquad P(A \cap B) = 40\%$$
$$P(A \cap B \cap C) = 12\%, \qquad P(A \cup B) = 85\% \text{ etc.}$$

while the percentage of the children taking none of the subjects A, B, C is

$$P(\tilde{A} \cap \tilde{B} \cap \tilde{C}) = 14\%.$$

Consider now the four percentages:

$$P(A) = 75\% \qquad P(B) = 50\%$$
$$P(A \cup B) = 85\% \qquad P(A \cap B) = 40\%.$$

Among these numbers there is the relation

$$P(A)+P(B) = P(A\cap B)+P(A\cup B).$$

This is in fact a quite general relation, as we can prove by entering arbitrary figures in the primary regions of the Venn diagram. Thus, still working in percentages, suppose the diagram is

	B	
A	*l*	*m*
	n	*k*

$$l+m+n+k = 100.$$

Then
$$P(A) = (l+m)\%, \qquad P(B) = (l+n)\%$$
$$P(A\cup B) = (l+m+n)\%, \; P(A\cap B) = l\%,$$

giving the basic relation, which is usually written as

$$\text{I} \qquad P(A\cup B) = P(A)+P(B)-P(A\cap B).$$

8.3. *Probabilities*

The next phase of the problem is this: suppose a card is picked at random out of the 100 cards in the card-index; what is the probability that it is the card belonging to a child studying subject A? We take, in this context, the unsophisticated view of probability, namely, that since we know that 75 per cent of the children are studying subject A, we have a 75 per cent probability (i.e., a $\frac{3}{4}$ probability, which is a 3-to-1 chance) that the card belongs to a child who is studying subject A. We may therefore without ambiguity use the symbols we have already adopted and write

$$P(A) = 0.75 \text{ (rather than } 75\%).$$

Thus we have

$$P(A\cap B) = 0.40, \; P(A\cup B) = 0.85 \text{ etc.},$$

and the relation

$$\text{I} \qquad P(A\cup B) = P(A)+P(B)-P(A\cap B)$$

continues to be valid with this new interpretation of the symbol 'P'. This is therefore a basic relation among PROBABILITIES.

Suppose next that the cards had already been sorted on subject A, so that we have 75 cards in the A-pile and 25 in the $\bar{A}$-pile, and we wish to know the probability that a card selected at random from the A-pile refers to a child studying subject B. We sort the A-pile into a $(A \cap B)$-pile and a $(A \cap \tilde{B})$-pile, there being, on the figures we have assumed, 40 cards in the $(A \cap B)$-pile. That is, the probability that a child, already known to be studying subject A, should also be studying subject B is $\frac{40}{75} = 0.53$.

In general terms, this statement is written

$P(B|A)$: '*the probability of* B *given* A'. In terms of the general diagram

	B	
A	l/N	m/N
	n/N	k/N

$$l+m+n+k = N$$

$$P(B|A) = \frac{l}{l+m} = \frac{l/N}{(l+m)/N} = \frac{P(A \cap B)}{P(A)},$$

giving the relation

$$\text{II} \qquad P(B|A) = \frac{P(A \cap B)}{P(A)}.$$

8.4 *Independent probabilities*

The next question is: can we adapt the binary algebra to represent relations among probabilities? Suppose we write

$$X = P(A), \quad Y = P(B), \text{ etc.,}$$

where now $0 \leq X \leq 1$, $0 \leq Y \leq 1$. Can we find functions $m(X, Y)$ and $u(X, Y)$ which represent $P(A \cap B)$ and $P(A \cup B)$?

First we see that relation I gives

$$X+Y-m(X, Y) = u(X, Y),$$

which corresponds to the relation in the modified binary algebra of §7.6

$$x+y-m(x, y) = u(x, y)$$

since in that algebra $m(x, y) = xy$.

In what circumstances therefore is

$$m(X, Y) = XY?$$

In the case of the children taking subjects A and B this is clearly not true, since for that system, $X = P(A) = 0.75$, $Y = P(B) = 0.50$, $m(X, Y) = P(A \cap B) = 0.40$, while $XY = 0.375$.

In the general case, given by the diagram

	B	
A	l/N	m/N
	n/N	k/N

$$l+m+n+k = N$$

$$m(X, Y) = P(A \cap B) = l/N$$

while

$$XY = \frac{(l+m)(l+n)}{N^2}$$

$$\begin{aligned} m(X, Y)-XY &= [l(l+m+n+k)-(l+m)(l+n)]/N^2 \\ &= (lk-mn)/N^2, \end{aligned}$$

a quantity which, according to the values of l, m, n, k can be positive or negative, and is zero only when $m(X, Y) = XY$.

In what circumstances then is $m(X, Y) = XY$? Consider a quite different universal set from any we have discussed so far. Let U consist of all the combinations of a toss of a coin with a throw of a die, that is, the set that can be written as

$$\begin{aligned} U = \{&(H, 1), (H, 2), (H, 3), (H, 4), (H, 5), (H, 6), \\ &(T, 1), (T, 2), (T, 3), (T, 4), (T, 5), (T, 6)\}. \end{aligned}$$

U is the Cartesian product $C \times D$ of the sets of coin-tossings C and dice-throwings D.

Now dissect U by the statements

p_H: the result of the toss is a Head,
p_S: the result of the throw is a Six,

yielding the diagram:

	S	not−S
H	H6	H1 H2 H3 H4 H5
T	T6	T1 T2 T3 T4 T5

;

we have

$$\begin{aligned} p(\mathrm{H}) &= \tfrac{1}{2} \\ p(\mathrm{S}) &= \tfrac{1}{6} \\ p(\mathrm{H} \cap \mathrm{S}) &= \tfrac{1}{12}. \end{aligned}$$

Let us refer now to any act like the throwing of a die as an 'experiment', and the result of the act, such as scoring a '6' with the die, as an 'outcome of the experiment'. Suppose then that the experiment has m possible different outcomes (as the scoring of 1, 2, 3, 4, 5 or 6 on the die are the six possible outcomes of the experiment of throwing the die) and that these are all 'equally likely' (in the sense that with a properly constructed die properly thrown all six outcomes are equally likely). Finally let us assume r of these outcomes are to be accounted 'favourable' (as the throwing of a '6' might be so accounted, giving $r = 1$ favourable outcome). Then the probability of a favourable outcome of the experiment is $\mathrm{P(A)} = \dfrac{r}{m}$, where A stands for the set of favourable outcomes.

Now take a second quite distinct experiment, with n outcomes, s of them accounted favourable, so that

$\mathrm{P(B)} = \dfrac{s}{n}$, B being the set of favourable outcomes of this experiment.

Finally, let an 'experiment pair' consist of the completing of one experiment of each type. The universal set now consists of the mn possible joint outcomes of these experiment pairs; of these:

rn belong to subset A in which the outcome of the first type of experiment is successful, and

sm belong to subset B, and

rs belong to both A and B.

The set of outcomes can therefore be represented on the diagram:

	B	
A	rs	$r(n-s)$
	$(m-r)s$	$(m-r)(n-s)$

Thus

$$\mathrm{P(A \cap B)} = \frac{rs}{mn} = \frac{r}{m} \times \frac{s}{n}.$$

Two sets of experiments such as we have described, where there is a definite number of outcomes to each experiment and the outcome of an experiment in one set has no influence whatever on the outcome of an experiment in the other, are described as 'independent'. We have obtained the general result:

If two sets of experiments are independent, and the proportions of favourable outcomes of the experiments in the two sets are respectively P(A), P(B), then the probability of a favourable outcome to both experiments of a pair drawn one from each set is $P(A) \times P(B)$.

Usually we refer to 'events' rather than to 'favourable outcomes to experiments', and then replace the statement above by 'If two independent events occur separately with probabilities P(A), P(B), the probability that both events will occur is $P(A) \times P(B)$'. The word 'independent' is of course essential to the statement, and our line of argument applies only in the restricted circumstances that we have described.

8.5 *A proposed model which proves to be inconsistent*

We have found a special set of circumstances in which we may take a mathematical model with $P(A) = X$, $0 \leq X \leq 1$; $P(B) = Y$, $0 \leq Y \leq 1$ (so that $X^2 \leq X$, $Y^2 \leq Y$) and

$$m(X, Y) = XY$$

and $$u(X, Y) = X+Y-XY.$$

Is it possible to extend the use of this model? Let us assume that there are three independent events with probabilities

$$P(A) = X,\ P(B) = Y,\ P(C) = Z,$$
$$P(A \cap B) = XY,\ P(A \cap B \cap C) = P[(A \cap B) \cap C] = XYZ.$$

But now, $P[(A \cap B) \cap (A \cap C)] = XY \times XZ = X^2YZ \leq XYZ$, whilst $(A \cap B) \cap (A \cap C) \hat{=} A \cap B \cap C$.

It is clear what has gone wrong: the joint probability of two events of separate probabilities R and S is RS only when the events are independent. In the case above, we were given $A \cap B$ and C happen independently, so that $P[(A \cap B) \cap C] = XYZ$, but $A \cap B$ and $A \cap C$ are, by their very definition, not independent, so that the probability of the joint event $(A \cap B) \cap (A \cap C)$ is *not* the product of the probabilities of the separate events $(A \cap B)$ and $(A \cap C)$. No useful purpose can therefore be served by trying to evolve a model for probabilities on these lines.

We have the relation

$$u(X, Y) \equiv X+Y-m(X, Y)$$

and cannot go beyond this.

Exercise 1. Prove (i) $P(A-B) = X-m(X, Y)$.
(ii) $P(A+B) = u(X, Y)-m(X, Y)$.

8.6 *Characteristic functions and probabilities*

Let us take again the class of 24 children and write their initials on a Venn diagram under the classifications Girls (Boys) Right-handed (Left-handed) with Spectacles (not with Spectacles)—for the present purpose three more of the children are supposed to wear spectacles:

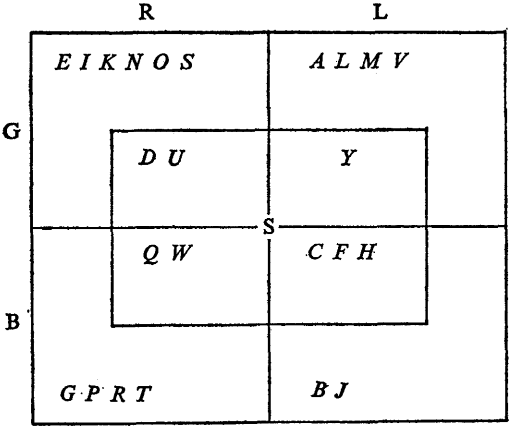


Diagram I

The numbers of children in various classifications and the 'probabilities' are:

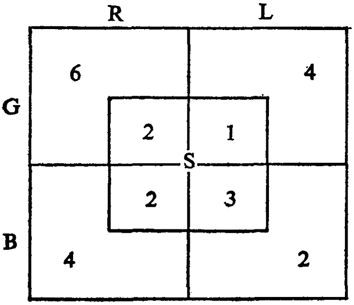


Diagram II

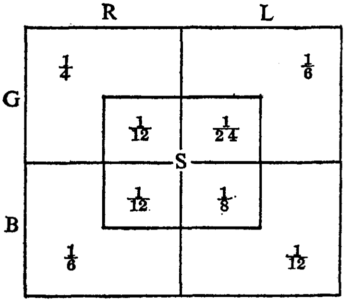


Diagram III

e.g., the probability that a child selected at random from the class should be a left-handed boy wearing spectacles is $\frac{1}{8}$.

Suppose next we are asked on the basis of diagram III what is the probability that a child selected at random is left-handed. In full the process of producing the answer would be first to reconstruct a diagram similar to II which shows that there are 10 such children out of 24. Thus the probability is $\frac{5}{12}$, a result we could have obtained directly by summing the probabilities $\frac{1}{6}+\frac{1}{24}+\frac{1}{8}+\frac{1}{12}$ in the L region of diagram III.

As a next step, suppose we are given not the numbers of children in each primary subset under the three classifications but the numbers in the following subsets:

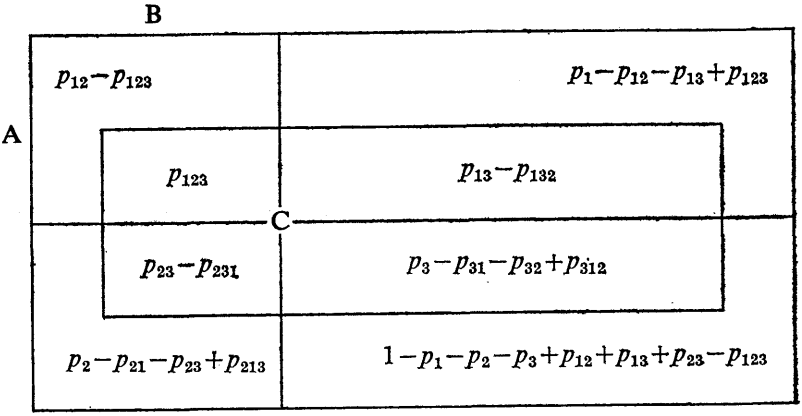
		Number	Probability
All children	(U)	24	1
Girls	(G)	13	$\frac{13}{24}$
Right-handed children	(R)	14	$\frac{7}{12}$
Right-handed girls	($G \cap R$)	8	$\frac{1}{3}$
Spectacle-wearers	(S)	8	$\frac{1}{3}$
Spectacle-wearing girls	($G \cap S$)	3	$\frac{1}{8}$
Right-handed spectacle-wearers	($R \cap S$)	4	$\frac{1}{6}$
Right-handed spectacle-wearing girls	($G \cap R \cap S$)	2	$\frac{1}{12}$

From these we could infer the numbers in all other subsets by filling in the entries in the diagram, starting with $G \cap R \cap S$ and working up the list.

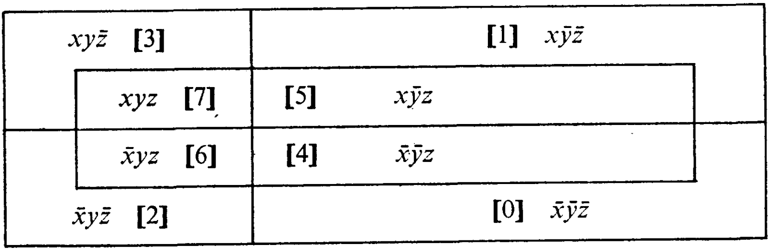
Let us now frame this in general terms:

Subset	Probability
U	1
A	p_1
B	p_2
$A \cap B$	$p_{12}\ (= p_{21})$
C	p_3
$A \cap C$	p_{13}
$B \cap C$	p_{23}
$A \cap B \cap C$	$p_{123}\ (= p_{213} = p_{312} =$ etc.)

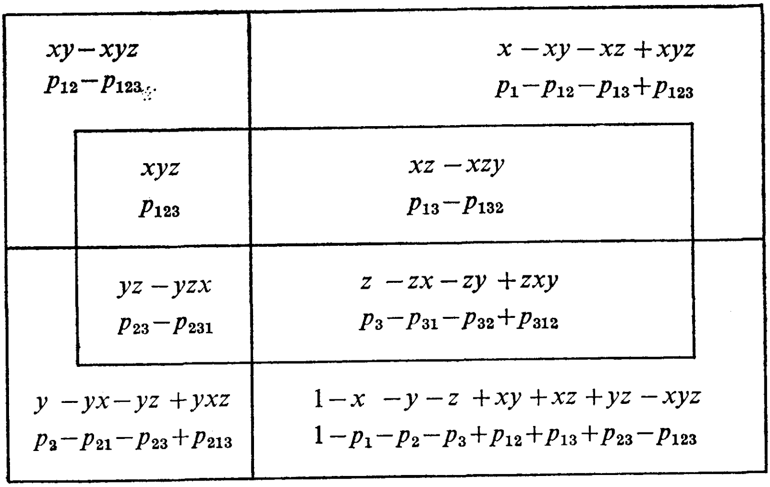
The corresponding diagram is:


B
A
C
$p_{12}-p_{123}$
$p_1-p_{12}-p_{13}+p_{123}$
p_{123}
$p_{13}-p_{132}$
$p_{23}-p_{231}$
$p_3-p_{31}-p_{32}+p_{312}$
$p_2-p_{21}-p_{23}+p_{213}$
$1-p_1-p_2-p_3+p_{12}+p_{13}+p_{23}-p_{123}$

Compare this with the characteristic function diagram (end of §7.3)



and write these two together, using the rational characteristic functions



From the discussion in §7.7, we know that the characteristic function of a subset is the sum of the characteristic functions of its constituent primary subsets; from the discussion above, we know that the probability that an element should belong to a subset is the sum of the probabilities of its belonging to the constituent primary subsets. From the last diagram, on writing x_1, x_2, x_3 for x, y, z, we see that if the rational characteristic function of a primary subset is

$$\alpha_0+\Sigma\alpha_i x_i+\Sigma\alpha_{ij}x_i x_j+\alpha_{123}x_1 x_2 x_3$$

where each α is either $+1$ or -1 or 0, then the probability that an element will belong to that primary subset is

$$\alpha_0+\Sigma\alpha_i p_i+\Sigma\alpha_{ij}p_{ij}+\alpha_{123}p_{123}.$$

Thus stated in general terms, the complete theorem is:

If in the dissection of a set by the subsets A_1, A_2, ..., A_n the probability that an element belongs to the subset $\mathrm{A}_i \cap \mathrm{A}_j \cap \ldots \cap \mathrm{A}_k$ is $p_{ij\ldots k}$, then the probability that an element belongs to the subset F of which the rational characteristic function is

$$f(\mathbf{x}) \equiv \Sigma\alpha_{rs\ldots t}x_r x_s\ldots x_t$$

is

$$\Sigma\alpha_{rs\ldots t}p_{rs\ldots t}.$$

For example, let the index number of the subset F in a three-way classification of a set U be 134, i.e., let the subset be {[1], [2], [7]}; this has characteristic function

$$x+y-2xy-xz-yz+3xyz.$$

So that the probability that a randomly selected member of the set belongs to this set is

$$p_1+p_2-2p_{12}-p_{13}-p_{23}+3p_{123}.$$

In particular, if in the case of the class of 24 children, we seek the probability that a child is either

a left-handed girl without spectacles,
or a right-handed girl with spectacles,
or a right-handed boy without spectacles,

we shall find the probability to be

$$\tfrac{13}{24}+\tfrac{7}{12}+2.\tfrac{1}{3}-\tfrac{1}{8}-\tfrac{1}{6}+3.\tfrac{1}{12} = \tfrac{10}{24}.$$

In this case we could have obtained the result directly from diagram III which gives the probabilities of the primary subsets, namely,

$$\tfrac{1}{6}+\tfrac{1}{12}+\tfrac{1}{6} = \tfrac{5}{12}.$$

Exercise 2. Find in terms of the probabilities p_i, p_{ij}, p_{123} the probability that a random-selected member of the set under a three-way classification shall belong to the subset with index number 234. Apply this to the case of the 24 children, and check your result against the probabilities in diagram III. In terms of the classifications of the children, what is the briefest description of the subset with index number 234?

Exercise 3. An experiment consists of three independent operations:
Selecting a card from a set of five, 2 of which are Red and 3 Black;
Selecting a day of the week;
Tossing a die.

The set U, of 5 × 7 × 6 outcomes, is dissected by the classifications:
R : selecting a Red card;
S : selecting Saturday or Sunday;
T : tossing a Two.

Construct the diagram showing the probabilities of the primary subsets.

A subset F of U has as its rational characteristic function the function $f(x, y, z)$. Show that the probability that the result of the experiment will correspond to F is $f(\frac{2}{5}, \frac{2}{7}, \frac{1}{6})$, and illustrate by the case when F has index number 234.

Exercise 4. (See appendix to Chapter 7.) In a dissection of a set by two subsets show that the probability that an element belongs to the subset with index sequence (w_0, w_1, w_2, w_3), (§6.4), is

$$[1, p_1, p_2, p_{12}] \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} w_0 \\ w_1 \\ w_2 \\ w_3 \end{bmatrix}$$

Write down the corresponding expression for a dissection by three subsets.

II. ALLOWING FOR IGNORANCE

8.7 *An analysis of the physical problem*

Perhaps the main interest of this section lies in the display of the interaction between the 'observations' on a physical system and the logical development of a mathematical system that is intended to provide a model for it. We shall find that we are not able to make the description of the physical system sufficiently clear in meaning to allow us to be certain of the properties we shall require in the mathematical model, but that, when we have specified the mathematical system completely, the model enables us to give more precision to the interpretation of our observations of the physical system.

To clarify our initial ideas, let us suppose that the observed physical system is again the children in the class, and that to each of them we had given two cards, one either white or yellow, and the other either red or green, but no record was kept. Some time later, the children are asked to show their cards, so that a list may be made, but some of the children have lost one or both their cards, and have no recollection of the colours. Let us assume the following list is made:

	White (A) or Yellow ($\tilde{A}$)	Red (B) or Green ($\tilde{B}$)		
Anne	W	R	$A^{\surd}$	$B^{\surd}$
Bill	Y	G	$A^{\times}$	$B^{\times}$
Charles		R	A^{0}	$B^{\surd}$
Dorothy	W	G	$A^{\surd}$	$B^{\times}$
Evelyn			A^{0}	B^{0}
Fred	Y	R	$A^{\times}$	$B^{\surd}$
Geoff	Y	G	$A^{\times}$	$B^{\times}$
Henry		G	A^{0}	$B^{\times}$
Isobel	W	R	$A^{\surd}$	$B^{\surd}$
Jack			A^{0}	B^{0}
Karen			A^{0}	B^{0}
Lucy	W		$A^{\surd}$	B^{0}
Mary	W	R	$A^{\surd}$	$B^{\surd}$
Nancy	W	G	$A^{\surd}$	$B^{\times}$
Olive		R	A^{0}	$B^{\surd}$
Percy	Y		$A^{\times}$	B^{0}
Quentin	W		$A^{\surd}$	B^{0}
Richard			A^{0}	B^{0}
Susan	W	R	$A^{\surd}$	$B^{\surd}$
Tom		G	A^{0}	$B^{\times}$
Una	Y		$A^{\times}$	B^{0}
Vera		G	A^{0}	$B^{\times}$
Warren	W	R	$A^{\surd}$	$B^{\surd}$
Yolande	Y	R	$A^{\times}$	$B^{\surd}$

The fourth and fifth columns correspond to new sets of cards that are given out, namely, a card marked

$A^{\surd}$ to each child who holds a white card
$A^{\times}$,, a yellow card
$B^{\surd}$,, a red card
$B^{\times}$,, a green card
A^{0} ,, neither a white nor a yellow card
B^{0} ,, neither a red nor a green card.

So that, if a child is given a card marked $\left\{\begin{matrix}A^{\surd}\\A^{\times}\end{matrix}\right.$ we know that he was originally given a $\left\{\begin{matrix}\text{white}\\\text{yellow}\end{matrix}\right.$ card, but that, if he is given a card marked A^{0}, we do not know whether his original card was white or yellow.

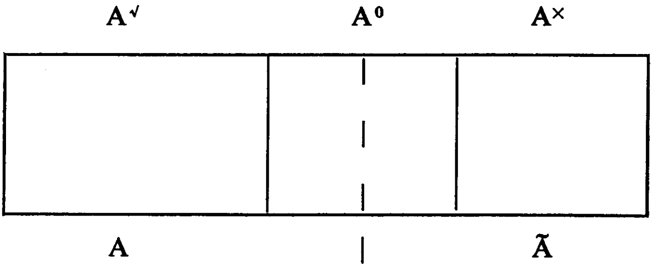
Now let us re-word this in terms of descriptive statements which determine subsets of a set U. A statement p_A (such as 'this child was originally given a white card') determines three mutually exclusive subsets:

$A^{\surd}$: $k \in A^{\surd}$ means we know that k satisfies the description p_A,
$A^{\times}$: $k \in A^{\times}$ means we know that k does not satisfy the description p_A, i.e., we know that k satisfies $p_{\tilde{A}}$,
A^{0} : $k \in A^{0}$ means that no information has been supplied as to whether or not k satisfies p_A.

Let us draw up lists of the children's initials under these three headings in the form of a modified Venn diagram.

$A^{\surd}$	A^{0}	$A^{\times}$
A D I *L M N* *Q S W*	*C E H* *J K O* *R T V*	*B F G* *P U Y*
We know that each of these children was given a white card.	We do not know for any of these children whether he was given a white card or a yellow card.	We know that each of these children was given a yellow card.

Underlying the subsets $A^{\surd}$, $A^{\times}$, A^{0} are the hypothetical subsets A and $\tilde{A}$ which would have been determined by p_A if we had had full information (that is, if no child had lost his card), so that we may superpose an 'ideal' diagram (one corresponding to perfect information) on the 'actual' diagram (corresponding to what we know) in the following way



but it has to be understood that we do not know of any member of A^{0} whether it belongs to A or $\tilde{A}$. It might well be that all members of A^{0} belonged to A and none to $\tilde{A}$ (i.e., that all children who had lost their white-or-yellow cards had been given white cards), so that the reader must not allow the diagram to mislead him.

From the diagram we see the following simple relations, which we take as the first set of axioms of the algebraic system that we are constructing:

A I $\quad (\widetilde{A^{\surd}}) \bumpeq A^{0} \cup A^{\times}, \quad (\widetilde{A^{0}}) \bumpeq A^{\surd} \cup A^{\times}, \quad (\widetilde{A^{\times}}) \bumpeq A^{\surd} \cup A^{0},$

A II $\quad (\tilde{A})^{\surd} \bumpeq A^{\times}, \quad (\tilde{A})^{\times} \bumpeq A^{\surd}, \quad (\tilde{A})^{0} \bumpeq A^{0},$

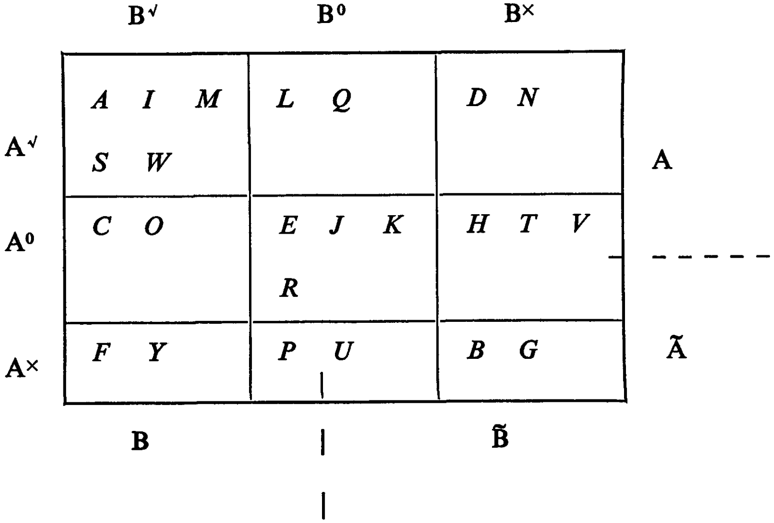
A III $\quad A^{\surd} \subseteq A, \quad A^{\times} \subseteq \tilde{A},$

A IV $\quad A^{\surd} \cup A^{0} \supseteq A, \quad A^{\times} \cup A^{0} \supseteq \tilde{A}.$

While, in terms of a physical system, the description 'the complement of the complement of A' leaves us with no doubt about the necessity for the property $\tilde{\tilde{A}} \bumpeq A$ in the corresponding abstract system, we cannot get a correspondingly clear idea from the physical system at present under consideration. One of the difficulties is that the physical system, described in terms of children retaining or losing cards, has been first interpreted as a system which is part verbal, part symbolic, namely, '$k \in A^{\surd}$' is equivalent to 'we know that $k \in A$' and '$k \in A^{0}$' to 'we have no information whether or not $k \in A$'.

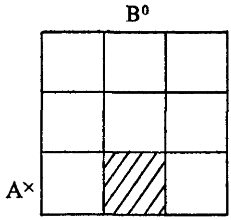
Corresponding to the relation $\tilde{\mathrm{A}} \bumpeq \mathrm{A}$ we have first to devise a meaning for $(\mathrm{A}^{\surd})^{\surd}$. In this case the meaning is fairly clear: $k \in (\mathrm{A}^{\surd})^{\surd}$ means 'we know that $k \in \mathrm{A}^{\surd}$' and so 'we know that we know that $k \in \mathrm{A}$', and, at its face value, this means '$k \in \mathrm{A}^{\surd}$'. But how should we interpret, say, $(\mathrm{A}^{\times})^{0}$? Expressed in words it is hard to see any meaning at all, and we shall have therefore to let the algebra take over. We shall have to devise, as we did in Chapter 7, algebraic forms (that is, characteristic functions) the values of which determine the relations of elements of the set to the dissecting subsets. The somewhat indeterminate phrases 'we know that $k \in \mathrm{F}$', 'we have no information about k in relation to F' will then be replaced by equations $f(x, y, z, \ldots) = 1, f(x, y, z, \ldots) = 0$, which express precisely that the elements for whose characteristic sequences the function f takes the value 1 or 0 belong respectively to $\mathrm{F}^{\surd}$ or F^{0}. We have to defer further discussion of this matter to §8.9.

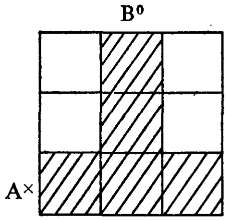
Let us now return to the analysis of the physical problem presented by the children and the coloured cards and draw up the lists of children's initials which form the modified Venn diagram for the double classification by p_A ('this child was given a white card') and p_B ('this child was given a red card').

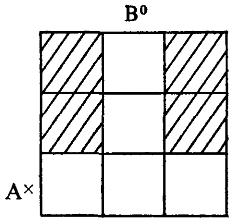


	$\mathrm{B}^{\surd}$	B^{0}	$\mathrm{B}^{\times}$
$\mathrm{A}^{\surd}$	*A I M S W*	*L Q*	*D N*
A^{0}	*C O*	*E J K R*	*H T V*
$\mathrm{A}^{\times}$	*F Y*	*P U*	*B G*

The two classifications and the state of our information in relation to them lead us therefore to 9 primary subsets. It is to be remembered that all the subsets we are considering are subsets in the sense in which we have been discussing them throughout the book, and we may carry out on them the set operations of complementation, union and intersection. So that, for example, $A^{\times} \cap B^{0}$, $A^{\times} \cup B^{0}$, $\widetilde{A^{\times} \cup B^{0}}$ are represented on the diagram respectively by the shaded regions:







We shall however find that we run into difficulties when we come to investigate the apparently empty set $A^{\surd} \cap A^{\times}$ and some others like it.

8.8 *Relations among subsets*

The two statements:

'We know the child *k* has a white card and we know the child *k* has a red card' and

'We know the child *k* has a white card and a red card' have the same meaning, that is

'We know that $k \in A$ and we know that $k \in B$' and

'We know that $k \in A \cap B$'

describe the same set of members of U, so that

A V $A^{\surd} \cap B^{\surd} \bumpeq (A \cap B)^{\surd}$.

While this relation seems to represent the physical situation that we have described when A and B are subsets determined by two descriptions which have no formal relation, we have to test its validity when B is replaced by either A or $\tilde{A}$. We find

$$A^{\surd} \cap A^{\surd} \bumpeq A^{\surd} \bumpeq (A \cap A)^{\surd},$$

and $$A^{\surd} \cap A^{\times} \bumpeq \varnothing \bumpeq (A \cap \tilde{A})^{\surd}$$

so that we may assume A V as one of the axioms of this system. We find later that in fact, while the axiom remains valid, we have to replace Ø in this context by a fictitious set A* which comes to play a significant but mysterious role in the analysis of the system.

In the same way, by reference to the last diagram, we see that we know that k satisfies at least one of the two logically unconnected descriptions p_A, p_B, if and only if we know that it satisfies the description $p_{A\cup B}$, so that we may assume

A VI $\qquad A^{\surd}\cup B^{\surd} \bumpeq (A\cup B)^{\surd}$.

If we replace B by A and $\tilde{A}$ we find

$$A^{\surd}\cup A^{\surd} \bumpeq A^{\surd} \bumpeq (A\cup A)^{\surd}$$

and

$$A^{\surd}\cup \tilde{A}^{\surd} \bumpeq A^{\surd}\cup A^{\times} \bumpeq U^{\surd} \bumpeq (A\cup \tilde{A})^{\surd}$$

where $U^{\surd}$, in relation to the single classification by A, is the subset of elements of U for which we have full information, i.e., if $k\in U^{\surd}$ we know whether k belongs to A or to $\tilde{A}$. In other words, $U^{\surd} \bumpeq \widetilde{A}^{0}$, namely, the complement of the subset about whose elements we have no information.

We may therefore adopt A VI, as well as A V, as an axiom of the system, but may have to modify the statement of some of the consequent relations in the light of further investigation.

Exercise 5. (i) Show the significance of these two axioms (A V and A VI) on the Venn diagram, putting in the children's initials.

(ii) Prove that

$$(A^{\surd}\cap B^{\surd})\cap C^{\surd} \bumpeq (A\cap B\cap C)^{\surd},$$
$$(A^{\surd}\cap B^{\surd})\cup C^{\surd} \bumpeq [(A\cap B)\cup C]^{\surd}.$$

(iii)

$$(A-B)^{\surd} \bumpeq A^{\surd}\cap B^{\times} \not\bumpeq A^{\surd}-B^{\surd},$$
$$(A+B)^{\surd} \bumpeq (A^{\surd}\cap B^{\times})\cup(A^{\times}\cap B^{\surd}) \not\bumpeq A^{\surd}+B^{\surd}.$$

Mark the corresponding regions on the Venn diagram.

The interpretation of $(A\cap B)^{\times}$ needs some consideration: we might argue that we have full knowledge of the relation of a member k of U to both propositions only when $k\in A^{\surd}\cap B^{\surd}$ or $A^{\surd}\cap B^{\times}$ or $A^{\times}\cap B^{\surd}$ or $A^{\times}\cap B^{\times}$, and, since $(A\cap B)^{\surd} = A^{\surd}\cap B^{\surd}$, this would lead us to define the subset $(A\cap B)^{\times}$ as the union of the last three of these four. But the proper interpretation of the symbol must be: $k\in(A\cap B)^{\times}$ if we know that k satisfies the proposition $\sim(p_A\cap p_B)$, i.e., $(\sim p_A\cup\sim p_B)$. Or, using the axioms already formulated,

$$\begin{aligned}(A\cap B)^{\times} &\bumpeq (\widetilde{A\cap B})^{\surd} \bumpeq (\tilde{A}\cup\tilde{B})^{\surd} \bumpeq \tilde{A}^{\surd}\cup\tilde{B}^{\surd}\\ &\bumpeq A^{\times}\cup B^{\times},\end{aligned}$$

which is another statement of the same relation. Similarly,

$$(A\cup B)^{\times} \bumpeq A^{\times}\cap B^{\times}.$$

Exercise 6. Prove that

$$(\mathrm{A}-\mathrm{B})^{\surd} \bumpeq (\mathrm{A}\,\sigma\,\mathrm{B})^{\times} \bumpeq \mathrm{A}^{\surd}\cap \mathrm{B}^{\times}$$
$$(\mathrm{A}-\mathrm{B})^{\times} \bumpeq \mathrm{A}^{\times}\cup \mathrm{B}^{\surd}$$
$$(\mathrm{A}+\mathrm{B})^{\times} \bumpeq (\mathrm{A}^{\surd}\cap \mathrm{B}^{\surd})\cup(\mathrm{A}^{\times}\cap \mathrm{B}^{\times}).$$

When our information is incomplete we should not expect to find a condition which is both necessary and sufficient. For example, suppose, in relation to the descriptions $\left\{\begin{matrix} p_A \\ p_{\tilde{A}} \end{matrix}\right.$: 'this child was given a $\left\{\begin{matrix} \text{white} \\ \text{yellow} \end{matrix}\right.$ card', we wish to test the validity of the statement: 'no child was given a white card', i.e.,

$$\mathrm{A} \bumpeq \varnothing.$$

Clearly, if any child still has a white card, then the statement is false, so that, interpreting now in terms of general sets,

$$\mathrm{A}^{\surd} \bumpeq \varnothing \text{ is necessary for } \mathrm{A} \bumpeq \varnothing.$$

On the other hand, we still do not know whether some of the children who have lost their cards were given white cards. Our only other certain information relates to children who still hold yellow cards, so that if $\mathrm{A} \bumpeq \varnothing$ then every child who still has a card has a yellow one, that is,

$$\mathrm{A} \bumpeq \varnothing \text{ is necessary for } \widetilde{\mathrm{A}^{\times}} \bumpeq \varnothing,$$

or expressing this as a sufficient condition

$$\mathrm{A}^{\surd}\cup \mathrm{A}^{0} \bumpeq \varnothing \text{ is sufficient for } \mathrm{A} \bumpeq \varnothing.$$

But from the information available we have no means of devising a condition that is both necessary and sufficient for $\mathrm{A} \bumpeq \varnothing$.

Exercise 7. Prove that

a necessary condition for $\mathrm{A}\subseteq\mathrm{B}$ is $\mathrm{A}^{\surd}\subseteq\mathrm{B}^{\surd}$,
a sufficient condition for $\mathrm{A}\subseteq\mathrm{B}$ is $(\mathrm{A}^{\surd}\cup \mathrm{A}^{0})\subseteq\mathrm{B}^{\surd}$.

Illustrate these conditions on the Venn diagram.

8.9 *Ternary algebra*

The next question is: can we invent an algebraic system to represent the relations among these new subsets corresponding to the binary algebra that we used in Chapter 7? The system we used there, namely, the algebra of odds and evens, that is, of remainders on division by 2, corresponds to the two-way division of U into a set and its complement. A likely line of approach then would appear to be to use the ternary algebra of remainders, 0, 1, -1, on division of integers by 3, for the components of the characteristic sequences and as the basis for a set of functions corresponding to the various set operations.

We assume then as our axioms the two tables:

$x+y$:

$x \backslash y$	1	0	-1
1	-1	1	0
0	1	0	-1
-1	0	-1	1

$x \times y$:

$x \backslash y$	1	0	-1
1	1	0	-1
0	0	0	0
-1	-1	0	1

for combining the numbers in this algebra, under the operations '+' and '×'.

It can be proved without difficulty that:
the operations '+' and '×' are commutative and associative, the operation '×' is distributive over '+' (but not vice versa). Also $x^3 \equiv x$ so that $x^{2r+1} \equiv x$, $x^{2r+2} \equiv x^2$, $r = 0, 1, \ldots$

We can select the numbers 1, 0, -1 to correspond to $k \in \mathrm{A}^{\surd}$, $k \in \mathrm{A}^{0}$, $k \in \mathrm{A}^{\times}$ in any way we please, and can determine the required functions accordingly. The most obvious arrangement is this: for an n-way classification under propositions $p_1, \ldots, p_n$ giving hypothetical subsets $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n$, we assign to each member k of U a characteristic sequence $(x_1, x_2, \ldots, x_n) = (x)$, in which each $x_i = 1, 0, -1$, in such a way that

$$x_i = 1 \text{ when } k \in \mathrm{A}_i^{\surd}$$
$$x_i = 0 \text{ when } k \in \mathrm{A}_i^{0}$$
$$x_i = -1 \text{ when } k \in \mathrm{A}_i^{\times}.$$

Alternatively, using the same rule for forming the characteristic sequences, we may assume as our axioms the axioms for the rational number system, and represent the relations among subsets:

(i) by constructing functions which, for the domain $\{1, 0, -1\}$ of each of the variables, have the range $\{1, 0, -1\}$, and

(ii) in carrying out algebraic operations, by replacing for each variable x, any odd power x^{2r-1} by x, and any even power x^{2r} by x^2 (because x^{2r+s} and x^s are indistinguishable for the prescribed domain).

Exercise 8. Prove that in this system:

$$(x^2 \pm x)^2 \equiv 2(x^2 \pm x),$$
$$(1+x)(1-x^2) \equiv (1-x)(1-x^2) \equiv (1-x^2)^2 \equiv 1-x^2.$$

In practice, although the manipulations involved are slightly more complicated, we use the rational system rather than the modulo 3 system, because coefficients which are rational numbers throw more light on the structure of expressions in which they occur than do the corresponding coefficients reduced modulo 3. For example, the coefficients $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$ which occur in the rational forms of some characteristic functions are more informative than the corresponding coefficients $-1, 1, -1, \ldots$ in the pure ternary algebra.

When there is a single classification, p_A, the statement 'x is the characteristic function of $\mathrm{A}^{\surd}$' means:

$x = 1 \Leftrightarrow k \in \mathrm{A}^{\surd}$ (we know that $k \in \mathrm{A}$)
$x = 0 \Leftrightarrow k \in \mathrm{A}^{0}$ (we have no information about k in relation to A)
$x = -1 \Leftrightarrow k \in \mathrm{A}^{\times}$ (we know that $k \notin \mathrm{A}$).

Interpreting this table from the bottom upwards, we see that $-x$ is the characteristic function of $\mathrm{A}^{\times}$, since $-x = 1 \Leftrightarrow k \in \mathrm{A}^{\times}$ (we know that $k \in \tilde{\mathrm{A}}$) etc.

The characteristic functions of U and Ø appear to be respectively 1 and -1, since they can be described in the following terms: 'we know of every element of $\begin{matrix}\mathrm{U}\\ \varnothing\end{matrix}$ that it $\begin{matrix}\text{belongs to every}\\ \text{does not belong to any}\end{matrix}$ non-empty subset'. These values are confirmed later.

By combining given subsets $\mathrm{A}^{\surd}$, A^{0}, $\mathrm{A}^{\times}$ we can construct at this stage altogether eight subsets, namely, Ø, $\mathrm{A}^{\surd}$, A^{0}, $\mathrm{A}^{\times}$, $\mathrm{A}^{\surd} \cup \mathrm{A}^{0}$, $\mathrm{A}^{\surd} \cup \mathrm{A}^{\times} \bumpeq \mathrm{U}^{\surd}$, $\mathrm{A}^{0} \cup \mathrm{A}^{\times}$, U. There are, however, altogether 27 functions $f(x)$ satisfying the required conditions (i) and (ii) above of domain, range and reduction of powers, namely, the functions of the form

$$ax^2+bx+c$$

which are such that

$$\begin{array}{lrl} \text{for } x = 1: & \left.\begin{array}{r} a+b+c = \alpha \\ c = \beta \\ a-b+c = \gamma \end{array}\right\} & \text{i.e., } \begin{array}{l} a = \frac{1}{2}(\alpha+\gamma)-\beta \\ b = \frac{1}{2}(\alpha-\gamma) \\ c = \beta \end{array} \\ \phantom{\text{for } x = {}} 0: & & \\ \phantom{\text{for } x = {}} -1: & & \end{array}$$

where α, β, γ take the values $1, 0, -1$ independently. 19 of these functions therefore have mathematical significance but at present no apparent significance in relation to the physical system of which the mathematical system is a model.

Five of the functions are 1, 0, -1, x, $-x$; the remaining 22 are

$x =$	1	0	-1	$x =$	1	0	-1
$f(x) =$	α	β	γ	$f(x) =$	α	β	γ
$\frac{1}{2}(x^2+x)$	1	0	0	$-\frac{1}{2}(x^2+x)$	-1	0	0
$1-x^2$	0	1	0	$-1+x^2$	0	-1	0
$\frac{1}{2}(x^2-x)$	0	0	1	$-\frac{1}{2}(x^2-x)$	0	0	-1
$\frac{1}{2}(-x^2-x+2)$	0	1	1	$\frac{1}{2}(x^2+x-2)$	0	-1	-1
x^2	1	0	1	$-x^2$	-1	0	-1
$\frac{1}{2}(-x^2+x+2)$	1	1	0	$\frac{1}{2}(x^2-x-2)$	-1	-1	0
$\frac{1}{2}(-3x^2+x+2)$	0	1	-1	$\frac{1}{2}(3x^2-x-2)$	0	-1	1
$\frac{1}{2}(3x^2+x-2)$	1	-1	0	$\frac{1}{2}(-3x^2-x+2)$	-1	1	0
$-(x^2+x-1)$	-1	1	1	x^2+x-1	1	-1	-1
$2x^2-1$	1	-1	1	$1-2x^2$	-1	1	-1
$-x^2+x+1$	1	1	-1	x^2-x-1	-1	-1	1

To find the characteristic function of A^0 we first select every function from this list which (i) takes the value 1 only when $x = 0$ and (ii) is symmetrically related to A and $\tilde{A}$, i.e., to $A^{\surd}$ and $A^{\times}$ and therefore takes the same value for $x = -1$ as for $x = 1$. There are only two such functions, namely, $1-x^2$ and $1-2x^2$; for only the first of these can a plausible case be made out in terms of statements about the physical system. Thus:

$$1-x^2 = \begin{cases} 1 & \text{for } x = 0, \text{ i.e., when } k \in A^0, \\ -1 & \text{never, i.e., we have no other certain information about } k, \\ 0 & \text{for } x = \pm 1, \text{ i.e., we have no information on the relation of } k \text{ to either A or } \tilde{A} \end{cases}$$

whilst

$$1-2x^2 = \begin{cases} 1 & \text{for } x = 0, \text{ i.e. when } k \in A^0 \\ 0 & \text{never, i.e., we have complete knowledge for every } k \\ -1 & \text{for } x = \pm 1, \text{ i.e., we know that either } k \in A^{\surd} \text{ or } k \in A^{\times}. \end{cases}$$

We assume therefore that the characteristic function of A^0 is

$$w(x) \equiv 1-x^2.$$

We have now

$i(x) \equiv x$: the characteristic function of $A^{\surd}$
$w(x) \equiv 1-x^2$: A^{0}
$\gamma(x) \equiv -x$: $A^{\times}$

Using these we can provide meanings for $(A^{\surd})^{\surd}$, $(A^{\surd})^{0}$, ..., symbols which can be written without ambiguity as $A^{\surd\surd}$, $A^{\surd 0}$, etc.

Characteristic function	Subset
$i(i(x)) \equiv x$	$A^{\surd\surd} \bumpeq A^{\surd}$
$w(i(x)) \equiv 1-x^2$	$A^{\surd 0} \bumpeq A^{0}$
$\gamma(i(x)) \equiv -x$	$A^{\surd\times} \bumpeq A^{\times}$
$i(\gamma(x)) \equiv -x$	$A^{\times\surd} \bumpeq A^{\times}$
$w(\gamma(x)) \equiv 1-x^2$	$A^{\times 0} \bumpeq A^{0}$
$\gamma(\gamma(x)) \equiv x$	$A^{\times\times} \bumpeq A^{\surd}$
$i(w(x)) \equiv 1-x^2$	$A^{0\surd} \bumpeq A^{0}$
$w(w(x)) \equiv 1-(1-x^2)^2 \equiv x^2$	$A^{00} \bumpeq A^{\surd} \cup A^{\times} \bumpeq U^{\surd}$
$\gamma(w(x)) \equiv x^2-1$	$A^{0\times} \bumpeq ?$

From the subsets named in the last column of this table we see that the only triple operations that need to be considered are those based on A^{00} and $A^{0\times}$. We find $A^{0\times\surd} \bumpeq A^{0\times}$, $A^{0\times\times} \bumpeq A^{0}$, $A^{0\times 0} \bumpeq A^{00}$, $A^{00\surd} \bumpeq A^{00}$, $A^{000} \bumpeq A^{0}$, $A^{00\times} \bumpeq A^{*}$, say, where the characteristic function of A^{*} is $-x^2$.

$$A^{*\surd} \bumpeq A^{*},\ A^{*0} \bumpeq A^{0},\ A^{*\times} \bumpeq A^{00}.$$

Thus the complete set of subsets needed to interpret the symbols $A^{\cdots}$ with multiple indices $\surd$, o, $\times$ is $A^{\surd}$, A^{0}, $A^{\times}$, A^{00}, $A^{0\times}$, $A^{00\times}$.

But now let us look more closely at $A^{0\times}$ and A^{*}, whose characteristic functions are x^2-1 and $-x^2$. For $x = 1, 0, -1$ neither of these functions can take the value 1, which is the condition that a member k of U should belong to the subset. In terms of the physical system therefore $A^{0\times}$ and A^{*} have no members. But neither of them is, in terms of their characteristic functions, the empty set $\emptyset$, the characteristic function of which (as we confirm later) is -1. Thus the subsets $A^{0\times}$ and A^{*} are 'fictitious' sets, not practically realisable, but having quite well defined mathematical relations to the mathematical representations of the subsets in the physical system. In these respects they are the exact analogue of complex roots of quadratic equations. We shall find more of these 'fictitious' subsets and shall discuss them in more detail later.

8.10 *Intersections and unions; tangible and fictitious subsets*

The principal functions to be determined are the characteristic functions corresponding to the nine primary subsets (i.e., the intersections of $A^{\surd}$, A^0 and $A^{\times}$ with $B^{\surd}$, B^0 and $B^{\times}$) and to the union of two subsets. In the physical system for which we are constructing the model the four primary subsets, $(A \cap B)^{\surd} \bumpeq A^{\surd} \cap B^{\surd}$, $(A-B)^{\surd} \bumpeq A^{\surd} \cap B^{\times}$, $(B-A)^{\surd} \bumpeq A^{\times} \cap B^{\surd}$ and $(\tilde{A} \cap \tilde{B})^{\surd} \bumpeq A^{\times} \cap B^{\times}$, are more clearly defined than the others, so that we use these to determine the forms of the characteristic functions corresponding to the operations of union and intersection. We can then test their application to the subsets consisting of elements about which we have incomplete information.

Let $\mu(x, y)$ be the characteristic function of the subset $(A \cap B)^{\surd}$, then, if the characteristic sequence of an element k is (x, y):

$$\mu(x, y) = \begin{cases} 1 & \text{when } k \in (A \cap B)^{\surd}, \text{ i.e., when } x = y = 1, \\ -1 & \text{when } k \in A^{\times} \cup B^{\times}, \text{ i.e., when either } x = -1 \\ & \quad \text{or } y = -1, \\ 0 & \text{otherwise.} \end{cases}$$

The table of values is therefore:

$A \cap B$: $\mu(x, y)$:

$x \backslash y$	1	0	-1
1	1	0	-1
0	0	0	-1
-1	-1	-1	-1

Since the function is symmetric in x and y and $x^3 \equiv x$, etc., the most general form of function of two variables that can be assumed is

$$\mu(x, y) \equiv a + b(x+y) + c(x^2+y^2) + dxy + exy(x+y) + fx^2y^2.$$

From the table of values we find

$$\begin{array}{rrl}
x & y & \qquad \mu(x, y) \\
0 & 0 & 0 = a \\
\begin{array}{r}0\\0\end{array} & \begin{array}{r}1\\-1\end{array} & \left.\begin{array}{rl}0 = & b+c\\ -1 = & -b+c\end{array}\right\} \quad \begin{array}{rl} b = & \frac{1}{2}\\ c = & -\frac{1}{2}\end{array} \\
1 & 1 & 1 = 2b+2c+d+2e+f
\end{array}$$

i.e.,
$$\left.\begin{aligned} 0 &= d+2e+f \\ 0 &= -d \quad +f \\ 1 &= d-2e+f \end{aligned}\right\} \quad \begin{aligned} d &= \tfrac{1}{2} \\ e &= 0 \\ f &= \tfrac{1}{2} \end{aligned}$$

$1 \quad -1$
$-1 \quad -1$

i.e.,

$$\begin{aligned} \mu(x, y) &\equiv \tfrac{1}{2}[(x-x^2)+(y-y^2)+(xy+x^2y^2)] \\ &\equiv \tfrac{1}{2}[(1+x)(1+y)+(1-x^2)(1-y^2)]-1. \end{aligned}$$

As special cases we have:

$(A \cap A)^{\surd}$: $\mu(x, x) \equiv x$,

corresponding to $(A \cap A)^{\surd} \bumpeq A^{\surd}$.

$(A \cap \tilde{A})^{\surd}$: $\mu(x, -x) \equiv -x^2$,

confirming that $(A \cap \tilde{A})^{\surd} \bumpeq A^{\surd} \cap A^{\times}$ is the fictitious subset A^*.

Exercise 9. Verify that:

$$A^{\surd} \cap A^* \bumpeq A^0 \cap A^* \bumpeq A^{\times} \cap A^* \bumpeq A^* \cap A^* \bumpeq A^*$$

and that $B^0 \cap A^* \bumpeq A^*$.

Exercise 10. Verify that $A^{\surd} \cap A^0$ and $A^{\times} \cap A^0$ are fictitious subsets with characteristic functions $-\frac{1}{2}(x^2-x)$, $-\frac{1}{2}(x^2+x)$ respectively.

We have found now several fictitious subsets, each corresponding to an algebraic expression derived from the intersection of a pair of subsets which is disjoint in the physical system. It is clear therefore that the mathematical system is more comprehensive than the system that we described in language appropriate to tangible objects. This extension of meaning is of the same nature as the extension which enriches geometry when we introduce co-ordinates. In real geometry a circle meets a line only if the line is not too far from its centre; in analytical geometry (over the complex field) every circle meets every line. In tangible set theory two subsets are such that they either do or do not have common members; in the system that we have devised, any two subsets determined by a simple classification have common members either 'tangible' or 'fictitious'.

Turning now to the function $v(x, y)$ corresponding to $A \cup B$, we have

$$v(x, y) = \begin{cases} 1 \text{ when } k \in (A \cup B)^{\surd} \bumpeq A^{\surd} \cup B^{\surd} \\ -1 \text{ when } k \in (A \cup B)^{\times} \bumpeq A^{\times} \cap B^{\times} \\ 0 \text{ otherwise,} \end{cases}$$

so that the table of values is:

$A \cup B : v(x, y)$

$x \backslash y$	1	0	−1
1	1	1	1
0	1	0	0
−1	1	0	−1

Comparing this table with the table for $\mu(-x, -y)$ we see that

$$v(x, y) \equiv -\mu(-x, -y) \equiv \tfrac{1}{2}[(x^2+x)+(y^2+y)-(xy+x^2y^2)]$$
$$\equiv 1-\tfrac{1}{2}[(1-x)(1-y)+(1-x^2)(1-y^2)].$$

Consider next the characteristic functions of U and Ø; from descriptions in the tangible system we expect these to be 1 and −1. We confirm these values by applying the functions $\mu(x, y)$, and $v(x, y)$ to the relations $A \cap U \hat{=} A$, $A \cup U \hat{=} U$, $A \cap \emptyset \hat{=} \emptyset$, $A \cup \emptyset \hat{=} A$, that is, by showing that

$$\mu(x, y) \equiv x \text{ and } v(x, y) \equiv y \quad \Rightarrow y = 1,$$
$$\mu(x, y) \equiv y \text{ and } v(x, y) \equiv x \quad \Rightarrow y = -1.$$

We have

	for U	for Ø
$2\mu(x,y) \equiv x+y-x^2-y^2+xy+x^2y^2$	$\equiv 2x$	$\equiv 2y$
$2v(x,y) \equiv x+y+x^2+y^2-xy-x^2y^2$	$\equiv 2y$	$\equiv 2x$
$\mu+v \equiv x+y$	$\equiv x+y$	$\equiv x+y$

The last relation is nugatory, but

		for U	for Ø
$v-\mu \equiv$	$x^2+y^2-xy-x^2y^2$	$\equiv y-x$	$\equiv x-y$
for $x = 1,1$	$-y$	$= y-1, \Rightarrow y = 1$	$= 1-y,$ −
for $x = 0,$	y^2	$= y, \Rightarrow y = 0$ or 1	$= -y, \Rightarrow y = 0$ or −1
for $x = -1,1$	$+y$	$= y+1,$ −	$= -1-y, \Rightarrow y = -1$

i.e., the characteristic functions of U and Ø are respectively 1 and −1.

Exercise 11. Verify that:

$$[v(x, y)]^2 \equiv \tfrac{1}{2}[(x^2+x)+(y^2+y)-xy(x+y)]$$

and thence that $(A \cup B) \cap A \hat{=} A$,
i.e., that $\mu[v(x, y), x] \equiv x$.

In the algebraic model we assume that the functional forms μ, v apply to the characteristic functions of any subsets, and we have already seen that this assumption leads to the postulation of fictitious subsets as the intersections of subsets whose tangible intersections are empty. From the three original subsets defined by a single classification p_A we find that we can derive altogether 17 subsets of which eight are tangible and nine fictitious. The characteristic functions of these subsets occur in pairs $f(x)$ and $-f(x)$, which we could describe as 'associated'. The following table lists these subsets:

	Subset F	Char. function $f(x)$	Values for $x =$			Associated subset $F^\times(-f(x))$	
			1	0	−1		
Tangible	$U \overset{\frown}{=} A^{00} \cup A^0$	1	1	1	1	$\emptyset \overset{\frown}{=} A^* \cap A^{0\times}$	Tangible
	$A^\surd$	x	1	0	−1	$A^\times$	
	A^0	$1-x^2$	0	1	0	$A^{0\times}$	Fictitious
	$A^\surd \cup A^\times \overset{\frown}{=} A^{00}$	x^2	1	0	1	$A^\surd \cap A^\times \overset{\frown}{=} A^*$	
	$A^\surd \cup A^0$	$1-\frac{1}{2}(x^2-x)$	1	1	0	$A^\times \cap A^{0\times}$	
	$A^\times \cup A^0$	$1-\frac{1}{2}(x^2+x)$	0	1	1	$A^\surd \cap A^{0\times}$	
Fictitious	$A^\surd \cap A^0$	$-\frac{1}{2}(x^2-x)$	0	0	−1	$A^\times \cup A^{0\times}$	
	$A^\times \cap A^0$	$-\frac{1}{2}(x^2+x)$	−1	0	0	$A^\surd \cup A^{0\times}$	
	$A^{00} \cap A^0 \overset{\frown}{=} \Theta$ say	0	0	0	0	Self.	

There are apparently many other combinations, for example, $(A^\surd \cup A^0) \cap A^\times$, but the reader will find that each of these reduces to one of those above.

The fictitious set Θ, which, having characteristic function 0, is independent of A, looks like another candidate for the empty set, but we see that it does not have the required properties. Its intersection and union with any subset B are not $\emptyset$ and B, but two fictitious subsets, namely,

$$B \cap \Theta \overset{\frown}{=} B^\surd \cap B^0, \text{ characteristic function } \tfrac{1}{2}(y-y^2),$$

$$B \cup \Theta \overset{\frown}{=} B^\surd \cup B^{0\times}, \text{ characteristic function } \tfrac{1}{2}(y+y^2).$$

Exercise 12. Verify that:

(i) $A^{\surd} \cup A^{*} \bumpeq A^{\surd}$, $A^{0} \cup A^{*} \bumpeq A^{0}$, $A^{\times} \cup A^{*} \bumpeq A^{\times}$;

(ii) $A^{\times} \cap (A^{0} \cup A^{\surd}) \bumpeq A^{\times} \cap A^{0}$;

(iii) $A^{0} \cup A^{0\times} \bumpeq A^{0}$, $A^{0} \cap A^{0\times} \bumpeq A^{0\times}$.

The characteristic functions of the ten compound subsets determined by A and B about which we have complete information are:

$A^{\surd} \cap B^{\surd} \bumpeq (A \cap B)^{\surd}$	$\mu(x, y)$
$A^{\surd} \cap B^{\times} \bumpeq (A - B)^{\surd}$	$\mu(x, -y)$
$A^{\times} \cap B^{\surd} \bumpeq (B - A)^{\surd}$	$\mu(-x, y)$
$A^{\times} \cap B^{\times} \bumpeq (A \downarrow B)^{\surd} \bumpeq (A \cup B)^{\times}$	$\mu(-x, -y)$
$A^{\surd} \cup B^{\surd} \bumpeq (A \cup B)^{\surd}$	$v(x, y) \equiv -\mu(-x, -y)$, etc.

Exercise 13. Complete this table by:

(i) writing in the characteristic functions of $(A \,\sigma\, B)^{\surd}$, $(B \,\sigma\, A)^{\surd}$, $(A \cap B)^{\times}$;

(ii) verifying from its table of values that the characteristic function of $(A + B)^{\surd}$ is $-xy$.

Exercise 14. Verify that the characteristic function of $(A \cap B \cap C)^{\surd}$ is

$$\mu(x, y, z) \equiv \tfrac{1}{4}(1+x)(1+y)(1+z)[1+(1-x)(1-y)+(1-x)(1-z)+(1-y)(1-z)]-1$$

and write down the corresponding form for $v(x, y, z)$.

These forms show clearly the advantage of not working with coefficients reduced modulo 3.

Finally we calculate the characteristic functions of the remaining five primary subsets (those about which we have incomplete information), under the assumption that the functional form is applicable. Let $\mu_{\surd 0}(x, y)$ be the characteristic function of $A^{\surd} \cap B^{0}$, then

$$\begin{aligned} \mu_{\ 0}(x, y) &\equiv \mu(x, 1-y^{2}) \\ &\equiv \tfrac{1}{2}[x+1-y^{2}-x^{2}-(1-y^{2})^{2}+x(1-y^{2})+x^{2}(1-y^{2})^{2}] \\ &\equiv x - \tfrac{1}{2}y^{2}(x^{2}+x). \end{aligned}$$

The table of values is

$\mu_{\surd 0}(x, y)$:

$x \backslash y$	1	0	−1
1	0	1	0
0	0	0	0
−1	−1	−1	−1

i.e.,
$$\mu_{\surd 0} = \begin{cases} 1 \text{ only when } k \in \mathrm{A}^{\surd} \cap \mathrm{B}^{0}, \\ -1 \text{ when } k \in \mathrm{A}^{\times}, \text{ i.e., when 'we know that } k \notin \mathrm{A}\text{'}, \\ 0 \text{ otherwise.} \end{cases}$$

Exercise 15. Write down the characteristic functions of $\mathrm{A}^{\times} \cap \mathrm{B}^{0}$ and $\mathrm{A}^{\surd} \cup \mathrm{B}^{0}$.

The only remaining primary subset is $\mathrm{A}^{0} \cap \mathrm{B}^{0}$, the characteristic function of which is given by

$$\mu_{00}(x, y) \equiv \mu(1-x^2, 1-y^2) \equiv (1-x^2)(1-y^2),$$

the table of values of which is

$\mu_{00}(x, y)$:

$x \backslash y$	1	0	−1
1	0	0	0
0	0	1	0
−1	0	0	0

This agrees with the physical interpretation, thus

$$\begin{aligned} \mu_{00}(x, y) &= 1 : k \in \mathrm{A}^{0} \cap \mathrm{B}^{0} \\ &= 0 \text{ in all other cases, i.e., we have no information on} \\ &\qquad k \text{ in regard to either A or B} \\ &= -1 \text{ never.} \end{aligned}$$

Exercise 16. Check that $v\{v[\mu_{\surd 0}(x, y), \mu_{\times 0}(x, y)], \mu_{00}(x, y)\} \equiv 1-y^2$ and comment on the result.

Exercise 17. Find the characteristic functions of $\mathrm{A}^{\surd} \cap \mathrm{B}^{*}$, $\mathrm{A}^{\surd} \cup \mathrm{B}^{*}$, $\mathrm{A}^{0} \cap \mathrm{B}^{*}$, $\mathrm{A}^{0} \cup \mathrm{B}^{*}$, $\mathrm{A}^{*} \cap \mathrm{B}^{*}$, $\mathrm{A}^{*} \cup \mathrm{B}^{*}$ and construct the tables of values.
Verify that $\mathrm{A}^{0} \cap \mathrm{B}^{*} \bumpeq \mathrm{B}^{*}$, $\mathrm{A}^{0} \cup \mathrm{B}^{*} \bumpeq \mathrm{A}^{0}$.

8.11 *Ordinary set relations and ternary algebra*

In this section we consider two ways in which the ternary algebra could be applied to the ordinary set relations and operations.

I Suppose that U is dissected by the set $\mathrm{A}^{+} \bumpeq \mathrm{A}^{\surd} \cup \mathrm{A}^{\times} \bumpeq \mathrm{U}_{A}^{\surd}$ where p_{A+} is 'we know the relation of k to the description p_A', e.g., A^{+} consists of the children who have retained their cards (and we are not concerned whether a card is white or yellow). The complementary set $\widetilde{\mathrm{A}^{+}} \bumpeq \mathrm{A}^{0}$.

In terms of the ternary algebra

$$k \in \mathrm{A}^{+} \Leftrightarrow x^2 = 1,$$
$$k \in \mathrm{A}^{0} \Leftrightarrow x^2 = 0.$$

The algebra appropriate to this system is therefore identical with that discussed in Chapter 7, except that the variables x, y, ... are replaced by x^2, y^2, ... While this system has therefore no intrinsic interest, it can be used to provide some check on the functional forms that were devised to represent operations with $\mathrm{A}^{\surd}$, A^{0}, $\mathrm{A}^{\times}$.

Exercise 18. (i) We have proved that the characteristic function of $(\mathrm{A}+\mathrm{B})^{\surd}$ is $-xy$. Show that the characteristic function of $(\mathrm{A}+\mathrm{B})^{\surd} \cup (\mathrm{A}+\mathrm{B})^{\times}$ is x^2y^2 and relate this to the statement above.

(ii) Consider also $\mathrm{A}^{0} \cap \mathrm{B}^{0}$, $\mu_{00}(x, y)$, and $m(x, y)$.

(iii) Verify that $\gamma(x^2) \equiv c(x^2)$, $\mu(x^2, y^2) \equiv m(x^2, y^2)$, $v(x^2, y^2) \equiv u(x^2, y^2)$, c, m, u being the rational characteristic functional forms.

II We shall obtain ordinary set-algebra from the algebra of $\mathrm{A}^{\surd}$, A^{0}, $\mathrm{A}^{\times}$ if we assume that the set A^{0} and all corresponding sets are empty, for in these circumstances $\mathrm{A}^{\surd} \mathrel{\hat{=}} \mathrm{A}$, $\mathrm{A}^{0} \mathrel{\hat{=}} \emptyset$, $\mathrm{A}^{\times} \mathrel{\hat{=}} \tilde{\mathrm{A}}$.

Thus we should be able to adapt the ternary algebra to the representation of Boolean algebra in a form in which the elements of the characteristic sequences are $+1$ and -1 according as the element concerned belongs to a subset or to its complement. Such a system would have the advantage that complementation was represented by change of sign.

We can construct such an algebra by picking out all those functions which take the value $+1$ or -1 for any primary subset for which the information is complete (i.e., subsets such as $\mathrm{A}^{\surd} \cap \mathrm{B}^{\times} \cap \mathrm{C}^{\surd}$ ...) and the value 0 for any other primary subset, i.e., one which is the intersection of sets one at least of which carries the 'no information' label ^{0}, such as $\mathrm{A}^{\surd} \cap \mathrm{B}^{0} \cap \mathrm{C}^{\times}$.

These functions $f(x_1, x_2, \ldots, x_r)$ have the value 0 whenever any variable $x_i = 0$, and either $+1$ or -1 when each variable x_i takes the value either $+1$ or -1. There is little to be gained by restricting the field of the coefficients to that of remainders on division by 3; the coefficients may be rationals, but the domain of the variables and the range of the functions are restricted to the set $\{1, 0, -1\}$; odd and even powers of a variable x are replaced respectively by x and x^2.

The basic functions relate to the unions and intersections of two sets, and their most general possible form is

$$a+bx+b'y+cx^2+c'y^2+xy(d+ex+e'y+fxy).$$

Since the value of the function is to be zero whenever either x or y is zero, we have

$$a = 0,\ \pm b+b' = 0,\ \pm c+c' = 0$$

and therefore $a = b = c = b' = c' = 0$. The only functions that have to be considered are therefore of the form

I $\qquad xy(d+ex+e'y+fxy)$

with the restriction that when the domain of (x, y) is $\{1, -1\}$, the range of the function is also $\{1, -1\}$. It appears that there are exactly 16 such functions corresponding to the set of subsets of a set under a double classification.

First, the functions corresponding to the simplest of subsets assume unexpectedly complicated forms; thus, for a single dissecting subset A, the characteristic functions of U and Ø are x^2 and $-x^2$. (When $\mathrm{A}^0 \doteqdot Ø$, $\mathrm{A}^{00} \doteqdot \mathrm{U}$ and $\mathrm{A}^* \doteqdot Ø$.) For two classifications U is represented by a function of the form I above which takes the value 1 for the four characteristic sequences $(\pm 1, \pm 1)$, so that $d = e = e' = 0$, $f = 1$, i.e., the characteristic function of U is x^2y^2. Since Ø is the complement of U the characteristic function of Ø is $-x^2y^2$. In the same way we find the characteristic function of A to be xy^2 and can complete the table for the six simplest subsets, namely,

U	A	$\tilde{\mathrm{A}}$	B	$\tilde{\mathrm{B}}$	Ø
x^2y^2	xy^2	$-xy^2$	x^2y	$-x^2y$	$-x^2y^2$

These are the functions for a two-way classification: for a dissection by n classifications the same form of analysis shows that the characteristic functions are

$\mathrm{U} : x_1^2 x_2^2 \ldots x_n^2$,
$\mathrm{A}_i : x_1^2 x_2^2 \ldots x^2_{i-1}\, x_i x^2_{i+1} \ldots x_n^2$, etc.

Exercise 19. The only other single-term functions of form I are $\pm xy$. Show that these correspond to A+B and its complement.

To find $\mu(x, y)$, the characteristic function of $\mathrm{A} \cap \mathrm{B}$, we have the equations

$$\begin{array}{lrcl}
(x, y) & \mu(x, y) & = & dxy+exy(x+y)+fx^2y^2 \\
1, 1 & 1 & = & d \quad +2e+f \\
1, -1 & -1 & = & -d \qquad +f \\
-1, -1 & -1 & = & d \quad -2e+f,
\end{array}$$

whence $d = \frac{1}{2}$, $e = \frac{1}{2}$, $f = -\frac{1}{2}$, and

$$\mu(x, y) \equiv \tfrac{1}{2}xy(1+x+y-xy) \equiv \tfrac{1}{2}xy(x+1)(y+1)-x^2y^2.$$

The remaining seven functions can be obtained from μ by sign changes (corresponding to the operation of complementation). The characteristic functions of the four primary subsets are:

$$\begin{aligned}
\mathrm{A} \cap \mathrm{B} &: \mu(x, y) \equiv \tfrac{1}{2}xy(x+1)(y+1)-x^2y^2 \\
\mathrm{A}-\mathrm{B} &: \delta(x, y) \equiv \tfrac{1}{2}xy(x+1)(y-1)-x^2y^2 \\
\mathrm{B}-\mathrm{A} &: \delta(y, x) \equiv \tfrac{1}{2}xy(x-1)(y+1)-x^2y^2 \\
\tilde{\mathrm{A}} \cap \tilde{\mathrm{B}} &: \nu(x, y) \equiv \tfrac{1}{2}xy(x-1)(y-1)-x^2y^2
\end{aligned}$$

As a check on the consistency of the system replace B by A in the first two functions.

$$\begin{aligned}
\mathrm{A} \cap \mathrm{A} \bumpeq \mathrm{A} : \mu(x, x) &\equiv \tfrac{1}{2}x^2(x+1)^2-x^4 \\
&\equiv \tfrac{1}{2}(x^2+2x^3+x^4)-x^4 \\
&\equiv x \text{ (since } x \equiv x^3,\ x^2 \equiv x^4) \\
\mathrm{A} \cap \tilde{\mathrm{A}} \bumpeq \varnothing : \mu(x, -x) &\equiv -\tfrac{1}{2}x^2(x^2-1)-x^4 \\
&\equiv -x^2.
\end{aligned}$$

These are the forms appropriate to a single classification; for a double classification we have

$$\begin{aligned}
\mu(xy^2, xy^2) &\equiv \tfrac{1}{2}x^2y^4(xy^2+1)^2-x^2y^4x^2y^4 \\
&\equiv \tfrac{1}{2}[x^2y^2+2x^3y^2+x^2y^2]-x^2y^2 \\
&\equiv xy^2, \text{ etc.}
\end{aligned}$$

The characteristic function of the union of two sets is given as in §8.10 by $v(x, y) \equiv -\mu(-x, -y) \equiv x^2y^2-\frac{1}{2}xy(x-1)(y-1)$.

Exercise 20. (i) Write down the characteristic function of $\mathrm{A}\ \sigma\ \mathrm{B}$.

(ii) Verify from the characteristic functions that $\mathrm{A} \cup \mathrm{A} \bumpeq \mathrm{A}$, $\mathrm{A} \cup \tilde{\mathrm{A}} \bumpeq \mathrm{U}$.

Now suppose that the subsets A, B are such that $\mathrm{A} \cap \mathrm{B} \bumpeq \varnothing$,

then $\qquad \frac{1}{2}xy(x+1)(y+1)-x^2y^2 = -x^2y^2$

i.e., $\qquad \frac{1}{2}xy(x+1)(y+1) = 0;$

the three admissible non-zero characteristic sequences are $(-1, 1)$, $(1, -1)$, $(-1, -1)$. In these circumstances $\mathrm{A} \cup \mathrm{B} \doteqdot \mathrm{A}+\mathrm{B}$; the corresponding relation for the characteristic functions is

$$[-\tfrac{1}{2}xy(x-1)(y-1)+x^2y^2]-[\tfrac{1}{2}xy(x+1)(y+1)] \equiv -xy,$$

i.e., $$v(x, y)-0 \qquad\qquad \equiv j(x, y).$$

From the primary subsets we may synthesise all the subsets in the set, and again there are some points in the detail of the algebra which should be noticed, because the same principles apply for many-way classifications. Thus, for example, corresponding to $(\mathrm{A} \cap \mathrm{B})+(\mathrm{A} \cap \tilde{\mathrm{B}})$ we have

$$-\mu\delta \equiv -[\tfrac{1}{2}xy(x+1)(y+1)-x^2y^2]\,[\tfrac{1}{2}xy(x+1)(y-1)-x^2y^2].$$

Write for the moment

$$t \equiv (x+1)(y+1), \quad t' \equiv (x+1)(y-1),$$

then $$x^2y^2tt' \equiv 0,$$

because this product includes the three factors y, $y+1$, $y-1$, and $y^3-y \equiv 0$.

So that
$$\begin{aligned} -\mu\delta &\equiv -\tfrac{1}{4}x^2y^2tt'+\tfrac{1}{2}x^3y^3(t+t')-x^4y^4 \\ &\equiv \tfrac{1}{2}xy(t+t')-x^2y^2 \\ &\equiv xy^2 \end{aligned}$$

(as it should, since $(\mathrm{A} \cap \mathrm{B})+(\mathrm{A} \cap \tilde{\mathrm{B}}) \doteqdot \mathrm{A}$).

The same reduction applies in the computation of the characteristic function of the union of any number of different primary subsets.

Exercise 21. The characteristic functions of three different primary subsets are $\tfrac{1}{2}xyt-x^2y^2$, $\tfrac{1}{2}xyt'-x^2y^2$, $\tfrac{1}{2}xyt''-x^2y^2$. Prove that the characteristic function of their union is

$$\tfrac{1}{2}xy(t+t'+t'')-x^2y^2.$$

(t, t', t'' are any three of the products $(x\pm 1)(y\pm 1)$).

For a three-way classification we shall find

$$\mu(x, y, z) \equiv \tfrac{1}{4}xyz(x+1)(y+1)(z+1)-x^2y^2z^2$$

since this function clearly takes the values:

0, whenever x or y or z is 0,
-1, whenever x or y or z is -1, and none of them is 0,
1, only when $x = y = z = 1$.

Exercise 22. (i) Prove that the characteristic function of the primary subset with characteristic sequence (i, j, k) is

$$\phi_{ijk}(x, y, z) \equiv \tfrac{1}{4}xyz[x-(-1)^i]\,[y-(-1)^j]\,[z-(-1)^k]-x^2y^2z^2.$$

(ii) Prove that, A, B, C, being the subsets determining the dissection, the characteristic function of A+B+C is xyz.

By the same method as we used for a two-way classification we find that the characteristic function of the subset which is the union of primary subsets with characteristic functions $\phi_{ijk}(x,y,z)$ for prescribed sequences (i, j, k) is

$$\tfrac{1}{4}xyz \sum_{i,j,k}[x-(-1)^i]\,[y-(-1)^j]\,[z-(-1)^k]-x^2y^2z^2$$

Exercise 23. Find the characteristic functions of the subsets with index numbers 134 and 234 in a three-way classification.

Chapter 9

NON-FINITE SETS—DENUMERABLE SETS

9.1 *The description 'non-finite'*

So far, all sets under consideration have been regarded as originating from collections of real objects, that is, collections that can be examined in full. Every object is present; the name of each element is present on a list of the elements of the set. Such collections and sets are termed 'finite'.

Sometimes a physically realisable collection, or perhaps a simply describable set, although finite, may in fact be so large that one would not consider for one moment the task of listing its elements. It may even happen that the size is so large that the task is beyond present technological resources even if utilised for a thousand years. In either case, one would still concede that such sets could be listed, given long enough time and sufficient paper.

Mathematics is, however, largely concerned with systems whose elements cannot be listed in the sense described above. Such systems, although suggested by physical considerations, are in effect creations of the human mind. 'Small' counting numbers are in everyday use, 'large' ones are common in, say, economic affairs, such as a national budget or an international corporation's balance sheet, 'very large' numbers are rarely used by anyone other than scientists and mathematicians. But the 'set of counting numbers' makes no concession for size; all the numbers described above are ordinary counting numbers, and rank as typical elements of that 'infinite set'.

We use the adjective 'non-finite' to describe such (mathematical) sets, mainly to free this account of any associations and connotations that the words 'infinite' and 'infinity' may have for the reader. In particular, we wish to dispel any illusion that 'infinity' is a number and '∞' its numeral. Also, we wish to avoid any specialised (but rather loose) use of 'infinity'. For example, physicists often regard everything outside a region of interest (be it an atom, a molecule, a tank of water, the earth, or the solar system) as being 'at infinity' if they wish to convey the idea that 'nothing outside the region of interest can produce a measurable change in the effect under observation'. Similarly, geometers have a 'line at infinity', which is simply a line singled out from all the lines in a plane to provide a definition of 'parallelism'.

9.2 *The idea of one-to-one correspondence*

If we look again at the transition from a collection of objects to a list of the names of the objects, we realise that we have used the obvious fact that there is a precise relationship between an object and its description. It will be remembered that we have always used distinguishable objects, and for the purpose of making a list we have named an object by referring to some quality which does distinguish it from the other objects in the collection.

For example, in the particular class we took as basic set U, we were able to identify the children either by the child's first name or by the initial letter of the child's first name. The identification is based on the following observation: to each child in U, there corresponds one first name and one initial letter; also, with each initial letter there is associated just one first name and just one child. Such a correspondence is called a one-to-one correspondence: it establishes a correspondence between two collections or sets in such a way that each element of one set corresponds to precisely one element of the other. Thus, with the list of first names and the list of initial letters used by us to describe the class, we had the one-to-one correspondence given by 'first name' corresponds to 'initial letter of first name'.

Some more examples:

(i) We cannot use the above one-to-one correspondence on the sets {*Anne*, *Alice*, *Bill*} and {A, B}. For '*Anne*' and '*Alice*' would both correspond to A, which clearly violates the condition that the correspondence be one-to-one.

Similarly, we fail if we try to set up a one-to-one correspondence (by the rule 'name' corresponds to 'surname') between the sets {*Anne Brown*, *Alice Brown*, *Bill Smith*} and {*Brown*, *Smith*}.

(ii) Consider the two sets {*a*, *b*, *c*} and {A, B, C, D}, and the correspondence of a small letter with its capital letter. Again, we cannot make it one-to-one, because there is no '*d*'.

In fact, a one-to-one correspondence between two finite sets is simply a pairing off of elements, one from each set, in such a way that the sets are exhausted simultaneously—there are no elements 'left over' from the pairing process.

We are quite accustomed to such processes in everyday life, so accustomed that usually it is quite simple for us to decide whether or not two collections have the 'same number of elements'. 'Number of elements' here means 'size', and we do not have to be able to count, nor to know any of the properties of counting numbers, in order to carry out the above process of pairing. Putting this another way, we can say of two given collections of objects whether one has more, fewer, or the same number of objects as the other (by pairing) but (until we have numbers) we cannot say how many objects each collection has.

The counting numbers may in this light be regarded as providing a standard reference set for the purpose of finding the number of objects in any one collection: we pair off the objects with the numbers 1, 2, 3, ... respectively until there are no objects left; the last counting number used is then the number of objects in the collection.

Thus, a set has five elements if it can be put in one-to-one correspondence with the set of numbers

$$S_5 \bumpeq \{1, 2, 3, 4, 5\}.$$

We shall denote the phrase 'is in one-to-one correspondence with' by the symbol $\simeq$, thus

$$\{a, b, c, d, e\} \simeq \{1, 2, 3, 4, 5\},$$

by say the pairing $(a, 3)$, $(d, 1)$, $(e, 2)$, $(c, 4)$ and $(b, 5)$.
[Note that pairing is not determined by the arrangement of elements within braces, for this is irrelevant as far as the set itself is concerned, and a one-to-one correspondence is a relation between sets.]

It is readily verified that:

(a) if $A \bumpeq B$ then $A \simeq B$, and so $A \simeq A$,
(b) if $A \simeq B$ then $B \simeq A$, and
(c) if $A \simeq B$, $B \simeq C$, then $A \simeq C$;

i.e., $\simeq$ is a reflexive, symmetric and transitive relation on (finite) sets.

A set A has fewer elements than a set B if it can be put into one-to-one correspondence with a proper subset of B, and we can express this as follows:

If $A \simeq S_m \bumpeq \{1, 2, \ldots, m\}$, and $B \simeq S_n \bumpeq \{1, 2, \ldots, n\}$, then 'A has fewer elements than B' means

$$S_m \subset S_n.$$

Suppose $A \simeq S_m$, $B \simeq S_n$, and we have $S_m \subseteq S_n$, $S_n \subseteq S_m$; i.e., A has at most as many elements as B, and B has at most as many elements as A. From this description we conclude that A and B have the same number of elements, and this agrees with the result

$$[S_m \subseteq S_n \text{ and } S_n \subseteq S_m] \Leftrightarrow [S_m \overset{\frown}{=} S_n].$$

9.3 *The counting or natural numbers*

It is not our intention to give a rigorous account of the development of natural (or counting) numbers, nor of the structure of the set o natural numbers. Such an account in a concise form is possible, but requires a level of mathematical understanding higher than that presumed so far in this book. We prefer to give an informal account of some avenues of investigation.

In studying how the natural numbers 1, 2, 3, ... have grown out of everyday handling of sets of elements, we can if we wish distinguish three ways in which they are used.

(a) *Counting:* all sets with 5 elements can be put into one-to-one correspondence with the set $S_5 \overset{\frown}{=} \{1, 2, 3, 4, 5\}$.

(b) *Counting combinations of sets:* if a set of 5 elements and another set of 3 elements, all elements being distinct, are combined into one set, that set has 8 elements. Results of this type correspond to the result

$S_n \overset{\frown}{=} \{1, 2, \ldots, n\} \simeq \{m+1, m+2, \ldots, m+n\} \overset{\frown}{=} S_{m+n} - S_n$ for any counting numbers n, m;

e.g., we pair off the first set with S_5, and the second set with $S_{5+3} - S_5 \overset{\frown}{=} \{6, 7, 8\}$, and form

$S_5 \cup (S_{5+3} - S_5) \overset{\frown}{=} \{1, 2, 3, 4, 5, 6, 7, 8\} \overset{\frown}{=} S_8$.

The algebraic properties of addition and multiplication of counting numbers correspond to the different ways of counting finite sets.

(c) *Given a set, arranging its elements in order:* we do this by using the 'natural order' 1, 2, 3, ... of the counting numbers to create an ordering of a set—we label its elements 'first', 'second', 'third', etc., if they are paired with 1, 2, 3, ... respectively. By doing this (i.e., by attaching a label specifying position), it is possible to distinguish originally identical objects, as for example we marked the equal factors of a number as 2_a, 2_b, 2_c, ... when discussing H.C.F. and L.C.M.

There is another interesting problem: given elements a, b, c, ..., what properties must they possess before they can be used as a substitute for the counting numbers? This problem effectively asks us to study the properties which characterise the counting numbers. We could ask for the simplest set of properties (axiom system) which enables elements a, b, c, ... to be used for counting, or ordering collections, or which enables the setting up of algebraic operations with properties similar to those of $+$ and $\times$.

Mathematical theories, such as those on Peano systems, cardinal numbers, order relations, ordinal numbers, various algebraic systems (e.g., the rational numbers, real numbers, abstract groups, rings and fields) have their ultimate origin in a study of one aspect or another of the natural numbers. Advances in mathematical logic, and a better understanding of the problems involved in setting up a logical theory of the number systems of mathematics have also resulted from studies of the counting numbers.

9.4 *The non-finite set* N *of counting numbers*

We shall take as basic example in the study of non-finite (or unlistable) collections the set $\mathrm{N} \triangleq \{1, 2, 3, \ldots\}$ of natural numbers. The first task is to discuss ways of describing or referring to subsets of N. Any finite subset, if not 'too large', can be specified by listing its elements, as e.g. {2, 5, 100, 10,000}; otherwise a descriptive statement, such as 'all elements of N between 10 and 1,000,000 (inclusive)' or 'all even numbers between 10^6+1 and $10^{10}+1$' enables us to decide whether a given element of N does or does not satisfy the relevant property. We could describe this last set more precisely in the form

$$\mathrm{P} \triangleq \{k : k = 2r,\ r \in \mathrm{N},\ 10^6+1<k<10^{10}+1\}.$$

Similarly, we may define any finite set of counting numbers either by giving a list of the members or by making a statement, p, of conditions which are satisfied by all the members of the set concerned and by no other numbers. The same formulation can be used for non-finite sets; thus

$$\{k : k \in \mathrm{N} \text{ and } k \text{ is even}\}$$

describes the set $\{2, 4, 6, 8, \ldots\}$;

$$\{k : k \in \mathrm{N} \text{ and } k \text{ is prime}\}$$

describes the set $\{2, 3, 5, 7, 11, 13, \ldots\}$;

since, for any $k \in \mathrm{N}$, we can decide whether or not k is even or a prime respectively.

There is one final remark to make: a phrase such as the 'set of all counting numbers' contains an essential contradiction. Unless a set is finite, you cannot write down, or name, or even think about 'all' its members, since 'all' necessarily carries with it an implication of some process of recognition which enables you to account for every one of the members of the set.

There is in fact the same reason for avoiding the use of 'all' in relation to a non-finite set as there is for avoiding 'infinite'. The word conjures up false and misleading images.

9.5 *Various methods for obtaining subsets of* N

We assume as known the algebraic properties of **N**, and also we suppose that the following extensions of **N** have been obtained:

$\mathbf{I} \triangleq$ set of integers.

$\mathbf{Q} \triangleq$ set of rational numbers.

$\mathbf{R} \triangleq$ set of real numbers.

Their algebraic properties will be assumed. The following properties of the real numbers can be found in standard works on elementary algebra.

1. The set **R** of real numbers consists of all decimals

$$\pm p_r p_{r-1} \ldots p_0 \cdot q_0 q_1 q_2 q_3 \ldots\ldots$$

where each of $p_r, \ldots, p_0, q_0, q_1, \ldots$ is one of the numbers 0, 1, 2, ..., 9, and the decimal expansion is either terminating or non-terminating. Any terminating decimal (i.e., one in which $q_j = 0$ for $j = \mathrm{N}, \mathrm{N}+1, \ldots$, for some $\mathrm{N} \geq 0$) can also be represented as a decimal in which $q_j = 9$ for $j = \mathrm{N}, \mathrm{N}+1, \ldots$.

2. Let q be a rational number, then q has a terminating decimal expansion if and only if $q = \frac{r}{s}$, where r and s are relatively prime and the distinct prime factors of s are 2 and 5 (or 2 or 5).

3. If x has a recurring decimal expansion, i.e.,

$$x = p_r p_{r-1} \ldots p_0 \cdot q_0 q_1 \ldots q_s b_1 b_2 \ldots b_k b_1 b_2 \ldots b_k b_1 b_2 \ldots b_k \ldots$$

where the block $b_1 b_2 \ldots b_k$ recurs, then x is a rational number.

4. If x is a rational number, then its decimal expansion is either a terminating or a recurring decimal.

5. If decimals with recurring 9's (see 1.) are excluded, then each

real number has a unique decimal expansion, and each decimal expansion represents a distinct real number.

Since the method of listing can be applied only to finite sets we have to devise other ways of prescribing non-finite sets. We can recognise three principal methods of prescription.

(a) *Prescription by a function*

We devise a rule which enables us to associate with each member of N some other member of N, the rule being such that the resulting set is non-finite. That is, we select a suitable function $f(x)$, such that

$$m \in \mathrm{N} \Rightarrow f(m) \in \mathrm{N},$$

and form the set

$$\mathrm{S} \bumpeq \{m' : m' = f(m), m \in \mathrm{N}\}.$$

It does not matter if not all the values $f(m)$ are distinct—we omit any repetitions.

Some examples of functions f are:

(i) $f(m) \equiv m^2$

$$\mathrm{S} \bumpeq \{1, 4, 9, 16, \ldots, m^2, \ldots\}.$$

(ii) $f(m) \equiv m^2 - 8m + 17$

$$\mathrm{S} \bumpeq \{10, 5, 2, 1, -, -, -, 17, 26, \ldots\},$$

where the mark '$-$' has been inserted to indicate the place of a number that has already appeared in the listing of the set so far as it has gone, but is irrelevant so far as the prescription of S is concerned.

(iii) The condition $f(m) \in \mathrm{N}$ would appear to restrict very severely our range of choice of functions, but we can circumvent this restriction by using instead of the calculated value of $f(m)$ the counting number $\phi(m) \equiv [1 + f(m)]$, where $[x]$ is the greatest integer less than or equal to x, that is, in the case when x is positive and expressed in the decimal scale as

$$x = p_r p_{r-1} \ldots p_0 \cdot q_1 q_2 \ldots,$$
$$[x] = p_r p_{r-1} \ldots p_0.$$

The term '1' has to be added to $f(m)$ because the least counting number is 1. For example,

$$f(m) \equiv m^{\frac{3}{2}}.$$
$$\phi(m) \equiv [1 + m^{\frac{3}{2}}].$$
$$\mathrm{S} \bumpeq \{2, 3, 6, 9, 12, 17, \ldots\}.$$

(iv) We require the set S determined by $\phi(m)$ to be completely determined, that is to say, when $\phi(m)$ is given, it is necessary that we should be able to say of any counting number m' either that it does or does not belong to S. While, in the case of the functions $f(m)$ above, this has been easy, it is not difficult to devise forms for $f(m)$ for which the actual determination could be quite a long process. For example, take

$$\phi(m) = [1+|m \sin(10m)^\circ|].$$

From trigonometric tables, we find for the successive values of $\phi(m)$, i.e., the members of S,

$$\mathrm{S} \overset{\frown}{=} \{1, -, 2, 3, 4, 6, 7, 8, 10, -, 11, -, -, -, 9, -, \ldots\}.$$

We see that for an arbitrary counting number r,

$$\phi(m) = 1 \qquad \text{when } m = 18r$$

and $\quad \phi(m) = m+1 \qquad \text{when } m = 18r+9$

with values between these for $18r<m<18r+9$.

Exercise 1. (i) Does $5 \in \mathrm{S}$?

(ii) Consider the sequences:

$$\phi(m) \equiv \left[1+\left|\tan\left(\frac{15\sqrt{2}}{8}\,m\right)^\circ\right|\right],$$

$$\psi(n) \equiv [1+|\tan(n \text{ radians})|].$$

In particular consider the values of $\phi(m)$ for $m = 34, 68, 102, 577$ and of $\psi(n)$ for $n = 11, 22$, and the behaviour of the functions at intermediate values.

For the present purpose it is sufficient to say that (given enough patience or a large enough computer) we can determine for any counting number m' whether there is a counting number m such that $\phi(m) = m'$. That is, we can say of any counting number m', either $m' \in \mathrm{S}$ or $m' \notin \mathrm{S}$. The set $\{m' : m' \notin \mathrm{S}\}$ is the complementary set $\tilde{\mathrm{S}}$ of S in precisely the same sense that we used this term for finite sets.

(b) *Prescription by an arithmetical property*

The method described in (a) certainly does not cover all subsets of N. For example, the notion of a 'prime' number depends on the multiplicative properties of N: p is a prime if, whenever $p = ab$ for $a \in \mathrm{N}$, $b \in \mathrm{N}$, then either $a = p$ or $b = p$. Given $m \in \mathrm{N}$, we can test each of the numbers $2, 3, \ldots, [\sqrt{m}]$ in turn as possible factors (a process which may take considerable time), and if none is, m is a prime. So the set of prime numbers is a well-defined subset of N. However, no one has yet devised a rule for specifying this subset (in the sense of method (a)). No one has proved that such a rule cannot exist, but we must be content with the specification $\{k : k \in \mathrm{N}$ and k is a prime$\}$ for the subset of primes. Many other simple problems in 'number theory' lead to subsets of N which are at present describable only by the statement of an arithmetical property. Indeed, often it is not known even if a given subset is finite or non-finite. For example, it is not known whether the set of 'prime pairs' i.e., pairs of numbers k, $k+2$ such that both k and $k+2$ are primes, is a finite or a non-finite set.

(c) *Prescription by a recurrence relation*

There is another method, similar to (a), which is sometimes used. This is the stating of a 'recurrence relation' which enables the successive determination of elements from the given values of a certain initial number. As examples:

(i) $u_n = u_{n-1}+u_{n-2}$ for $n \geq 3$, with $u_1 = u_2 = 1$, gives successively the numbers (the Fibonacci numbers)

$1, 1, u_3 = u_2+u_1 = 2, u_4 = u_3+u_2 = 3, u_5 = 5, u_6 = 8, \ldots,$

and the subset $\mathrm{F} \triangleq \{1, 2, 3, 5, 8, 13, \ldots\}$. Given $m \in \mathrm{N}$, we can determine whether, say, $m \in \mathrm{F}$ in one of the following ways. We observe that for $n>2$, $u_n>u_{n-1}$. Therefore there is only a finite number of elements of F which belong also to $\mathrm{S}_m \triangleq \{1, 2, \ldots, m\}$, so we calculate $u_1, u_2, \ldots$ successively until we come to the first value, say u_n, with $u_n>m$. Then if m is not one of $u_1, \ldots, u_n$, $m \notin \mathrm{F}$. Or, we may express u_n directly as a function $f(n)$ of n and seek if $m = f(n)$ has a solution for $n \in \mathrm{N}$. It can be proved that

$$u_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].^*$$

(ii) $\omega_n = (n-1)\,\omega_{n-1}+(n-1)\,\omega_{n-2}$ $(n \geq 3)$,

with $\omega_1 = 0$, $\omega_2 = 1$. This is the recurrence relation satisfied by the number of 'complete' permutations of n objects.

A 'permutation' of a finite set is simply a one-to-one correspondence of the set with itself. A permutation is complete if no element corresponds to itself (i.e., if no element is left 'fixed' by the correspondence). Again, since $\omega_n > \omega_{n-1}$ $(n \geq 2)$, we may decide of any element $m \in \mathrm{N}$ whether $m = \omega_n$ or not by finding $\omega_1, \omega_2, \ldots$ up to, say, ω_k, where k is the first element of N such that $\omega_k > m$.

---

* Linear recurrence relations such as $u_n = u_{n-1}+u_{n-2}$ were part of the stock-in-trade of examiners in mathematics in the period 1850 to 1910; the complete theory and many interesting examples can be found in many of the advanced algebra books of the period (e.g., Chrystal's *Algebra*, Chapter 31).

The function which expresses ω_n directly as a function of n is again quite complicated; it is

$$\omega_n = n!\left(\frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right).^*$$

While in these two cases it has been possible to replace the recurrence relation by a functional form, this is by no means generally the case. In many applications of mathematics the physical observations can be represented best by a mathematical model whose basis is a recurrence relation for which no exact equivalent functional form has yet been found. For example, a mathematical model for the growth of host-and-parasite populations under certain assumed environmental conditions can be based on such a recurrence relation.

Whatever method we adopt for prescribing a subset of N we assume that it leads to the following property:

Given S, a prescribed set, and m, an arbitrary counting number, then:

(i) one and only one of the two statements $m \in \mathrm{S}$ and $m \notin \mathrm{S}$ is valid,

(ii) in a finite number of steps we can determine which of the two statements is valid.

In consequence we can define the complement of S, namely, $\tilde{\mathrm{S}} \doteq \{m : m \notin \mathrm{S}\}$, and, for two prescribed sets S and T, the intersection,

$\mathrm{S} \cap \mathrm{T} \doteq \{m : m \in \mathrm{S} \text{ and } m \in \mathrm{T}\}$, and the union,

$\mathrm{S} \cup \mathrm{T} \doteq \{m : m \in \mathrm{S} \text{ or } m \in \mathrm{T}\}$.

Thus formally the algebra of operations on and relations among non-finite sets is identical with that for finite sets, i.e., with Boolean algebra.

9.6 *The relations* $\subset$ *and* $\simeq$ *between subsets of* N

From consideration of physically realisable collections of objects, we earlier drew the conclusion that if A and B are finite sets and

---

[*] E.g., Durell and Robson, *Advanced Algebra*, Chapters 11 and 18.

$B \subset A$, then A and B cannot be put into one-to-one correspondence; i.e., if A, B are finite subsets of N, and $B \subset A$, then $A \not\simeq B$. In particular, if $m, n \in N$, and $m \neq n$, then $S_m \not\simeq S_n$.

We introduce the symbol $\prec$ to denote the phrase 'can be put into one-to-one correspondence with a proper subset of' (if 'proper' is omitted, we use $\preceq$ instead of $\prec$). Then for any two finite subsets A, B, we have just one of the relations $A \prec B$, $A \simeq B$, or $B \prec A$, and this is true for any two finite subsets of N. In particular, we have

$$S_m \prec S_n \Leftrightarrow S_m \subset S_n,$$
$$S_m \simeq S_n \Leftrightarrow S_m \doteq S_n \Leftrightarrow m = n.$$

For non-finite subsets of N, it is not true that $A \subset B \Leftrightarrow A \prec B$. For example, let $B \doteq N$, and for A take the subset $\{2, 3, 4, \ldots\} \doteq N - \{1\}$. Then $A \subset B$, but $A \simeq B$ under the correspondence $n \in A \leftrightarrow n+1 \in B$, where the symbol $\leftrightarrow$ represents the phrase 'corresponds to'.* Thus '$n \leftrightarrow n+1$' means that the element n of A corresponds to the element $n+1$ of B which corresponds to the element n of A. To establish the relation $\leftrightarrow$ between the members of two sets is therefore to establish a one-to-one correspondence between the sets.

There is in fact a theorem that any non-finite subset of N can be put into one-to-one correspondence with N, that is,

$$[A \subseteq N \text{ and } A \not\simeq S_n \text{ (any } n \in N)] \Rightarrow A \simeq N.$$

To prove this we need to invoke the principle that we laid down earlier, namely, that the prescription of a subset A of N requires that, given any counting number m, we can determine in a finite number of steps that one and only one of the two statements $m \in A$ and $m \notin A$ is valid. We carry out this test successively for $m = 1$, $m = 2, \ldots$ and so arrive at a 'first' member of A, which we now label as a_1. Continuing the test we arrive at a 'second' member, a_2, and so on. That is, we establish a one-to-one correspondence between A and N in which $a_i \leftrightarrow i$, $a_i \in A$, $i \in N$. Thus, in a loose manner of expression, we may say 'Every non-finite subset of N has as many elements as N', meaning that the sets are in one-to-one correspondence.

It is not always a simple matter to find the 'first' element of an arbitrary subset A of N, nor can it be expected in general that the function $f(n) = a_n$ defined above has a simple form, such as a polynomial in n. The following examples should convince the reader.

---

* No confusion can arise from the use of the same symbol in Chapter 3 with a different meaning, since there it represented an operation on two statements.

Exercise 2. (i) If A $\simeq \{k : k = \phi(m)$ and $k \geq 5\}$, where

$$\phi(m) = [1+|m\sin(10m)^\circ|],$$

find the first and eighth elements when A is arranged in natural order. Is A a non-finite set?

(ii) Let A $\simeq \{k : k \in \mathbf{N}$ and $32k-15m = 1$ for some $m \in \mathbf{N}\}$. Find the least element of A (i.e., the first element of A when A is arranged in natural order).

9.7 *Denumerable sets*

We call a set A denumerable if it can be put into one-to-one correspondence with the set **N**. Thus the main result of §9.6 can now be written as: 'Any non-finite subset of **N** is denumerable'.

It is our intention now to show that certain familiar sets, each of which contains **N** as a proper subset, are denumerable. To achieve this, we must show that there is a one-to-one correspondence between each such set and **N**.

If we wish to specify a particular arrangement of the elements of a set A, we shall do so by use of the notation $<\ldots>$ instead of the notation $\{\ldots\}$. For example, if A $\simeq \{1, 2, 3, 4, 5\}$ then $<1, 2, 3, 4, 5>$ and $<1, 3, 5, 2, 4>$ denote respectively the arrangements 1, 2, 3, 4, 5 and 1, 3, 5, 2, 4 of the elements of A. Similarly, $<a_1, a_2, a_3, \ldots>$ denotes the arrangement, in the order shown, of the elements $a_1, a_2, \ldots$ of the non-finite set A.

The set **I** *of integers*

We take the arrangement $<0, 1, -1, 2, -2, \ldots, r, -r, \ldots>$ of **I** given by the one-to-one correspondence with **N** specified by the function

$$f(n) = 2n \qquad (n>0,\ n \in \mathbf{I}),$$
$$f(n) = -2n+1 \qquad (n \leq 0,\ n \in \mathbf{I}).$$

Hence **I** is denumerable, and so any non-finite subset of **I** is denumerable.

The set **P** *of counting number pairs*

P is the Cartesian product set **N** × **N**, and consists of all pairs (m, n) $m \in \mathbf{N}$, $n \in \mathbf{N}$. We exhibit the denumerability of **P** as follows.

For each $r \geq 2$, $r \in \mathbf{N}$, let

$$\Sigma_r \simeq \{(m, n) : (m, n) \in \mathbf{P},\ m+n = r\}.$$

Thus $\Sigma_3 \doteq \{(1, 2), (2, 1)\}$, $\Sigma_4 \doteq \{(1, 3), (3, 1), (2, 2)\}$.

We now specify an arrangement $<\Sigma_r>$ of Σ_r, by the rule: if (m, n) and (p, q) belong to Σ_r, then (m, n) precedes (p, q) if m precedes p in the arrangement $<1, 2, 3, \ldots>$ of **N**.
Thus $<\Sigma_r> \doteq <(1, r-1), (2, r-2), \ldots (s, r-s), \ldots (r-1, 1)>$.
Then the arrangement

$$<\mathbf{P}> \doteq <<\Sigma_2>, <\Sigma_3>, <\Sigma_4>, \ldots>$$

sets up a one-to-one correspondence between **P** and **N**.

Exercise 3. (i) Show that this one-to-one correspondence between **P** and **N** is given formally by the rule

$$f((m, n)) = \tfrac{1}{2}(m+n)(m+n+1)+m.$$

(ii) Verify that f is a one-to-one correspondence by showing:

(a) $[f((p, q)) = f((m, n))] \Rightarrow [(p, q) = (m, n)]$,

(b) if $k \in \mathbf{N}$, then $k = f((m, n))$ for some $(m, n) \in \mathbf{P}$.

The set $\mathbf{Q}^+$ *of positive rationals*

A number $x \in \mathbf{Q}^+$ if it is the solution of a linear equation

$$nx - m = 0$$

with $(m, n) \in \mathbf{P}$.

The correspondence $(m, n) \leftrightarrow x$ if $nx - m = 0$ is not one-to-one, for $(km, kn) \leftrightarrow x$ for any $k \in \mathbf{N}$. However, if we require that m and n are relatively prime, then the correspondence is one-to-one. Thus the set $\mathbf{Q}^+$ is equivalent to the subset

$$\mathbf{P}^{\#} \doteq \{(m, n) : m \# n\},$$

of **P**. Now (i) $\mathbf{P}^{\#}$ is not finite, since all elements $(p, 1)$, p a prime, belong to $\mathbf{P}^{\#}$. Therefore $\mathbf{P}^{\#}$ is a non-finite subset of the denumerable set **P**, and so is denumerable. $\mathbf{Q}^+$, being equivalent to $\mathbf{P}^{\#}$, is also denumerable.

Exercise 4. (i) Let $\Pi \doteq \mathbf{I} \times \mathbf{N} \doteq \{(m, n) : m \in \mathbf{I}, n \in \mathbf{N}\}$.
Show that Π is denumerable.

(ii) Let $\mathbf{Q} \doteq$ set of rationals $\doteq \{x : nx - m = 0, (m, n) \in \Pi\}$. Show that **Q** is equivalent to a non-finite subset of Π. Deduce that **Q** is denumerable.

(iii) Using the correspondences between **P** and **N**, and **I** and **N**, as models, devise a procedure which will enable you to arrange the elements of (a) $\mathbf{Q}^+$ and (b) $\mathbf{Q}$ in order. Exhibit the first ten elements of each arrangement. [Note that there is no first element of $\mathbf{Q}^+$ or of $\mathbf{Q}$ in the 'natural' ordering using $<$.]

(iv) Let x and y be rationals, and let $x<y$.
Show that if $z \in \mathbf{Q}$ lies between x and y, i.e., if $x<z<y$, then

$$z = (mx+ny)/(m+n)$$

for some element $(m, n) \in \mathbf{P}$, and conversely. Deduce that if

$$\begin{aligned} \mathbf{Q}(x, y) &\doteq \{\text{rationals between } x \text{ and } y\} \\ &\doteq \{k : k \in \mathbf{Q} \text{ and } x<k<y\}, \end{aligned}$$

then $\mathbf{Q}(x, y) \simeq \mathbf{N}$ for any two rationals x, y with $x<y$.

(v) By considering $f(x) \equiv x/(1-x)$, or otherwise, show that $\mathbf{Q}(0, 1)$ and $\mathbf{Q}^+$ can be put into a one-to-one correspondence F which preserves natural order, i.e., if $k_1, k_2 \in \mathbf{Q}(0, 1)$, then

$$[\mathrm{F}(k_1)<\mathrm{F}(k_2)] \Leftrightarrow [k_1<k_2].$$

(vi) By considering the function $f(x)$, defined on $-1<x<1$ by:

$$\begin{aligned} f(x) &= \frac{x}{1+x} && (-1<x<0), \\ f(x) &= 0 && (x = 0), \\ f(x) &= \frac{x}{1-x} && (0<x<1), \end{aligned}$$

deduce that any set $\mathbf{Q}(x, y)$ can be put into one-to-one natural order-preserving correspondence with $\mathbf{Q}$.

(vii) Show that there is no one-to-one correspondence between $\mathbf{Q}$ and $\mathbf{N}$ which preserves natural order.

9.8 *The set* $\mathbf{P}^*$ *of r-plets* ($r = 2, 3, \ldots$) *of counting numbers*

An element k of $\mathbf{P}^*$ is an element $(a_1, a_2, \ldots, a_r)$ of the r-fold Cartesian product $\mathbf{N}\times\mathbf{N}\times \ldots \times\mathbf{N}$ (r factors) for some $r \geq 2$. Let Σ_s^* be the subset of $\mathbf{P}^*$ consisting of those elements of $\mathbf{P}^*$ which satisfy the condition $a_1+a_2+\ldots+a_r = s$.
Then Σ_s^* is a finite set consisting of the duplets $(1, s-1)$, $(2, s-2)$, $\ldots$, the triplets $(1, 1, s-2)$, $(1, 2, s-3)$, $\ldots$, $\ldots$, and the s-plet $(1, 1, \ldots, 1)$. We can specify an arrangement $<\Sigma_s^*>$ of Σ_s^* thus:

a t-plet precedes a u-plet if $t<u$,

a t-plet $(a_1, \ldots, a_t)$ precedes a t-plet $(b_1, \ldots, b_t)$ if $a_1<b_1$, or $a_1 = b_1$ and $a_2<b_2$, or $a_1 = b_1$ and $a_2 = b_2$ and $a_3<b_3$, ...

That is, $(a_1, \ldots, a_t)$ precedes $(b_1, \ldots, b_t)$ if the first non-zero difference $a_1-b_1, a_2-b_2, \ldots, a_t-b_t$ is negative. Thus:

$$<\Sigma_2^*> \stackrel{\frown}{=} <(1, 1)>$$

$$<\Sigma_3^*> \stackrel{\frown}{=} <(1, 2), (2, 1), (1, 1, 1)>$$

$$\begin{aligned}<\Sigma_5^*> \stackrel{\frown}{=} &<(1, 4), (2, 3), (3, 2), (4, 1), (1, 1, 3), (1, 2, 2),\\ &(1, 3, 1), (2, 1, 2), (2, 2, 1), (3, 1, 1),\\ &(1, 1, 1, 2), (1, 1, 2, 1), (1, 2, 1, 1), (2, 1, 1, 1), (1, 1, 1, 1, 1)>.\end{aligned}$$

Then clearly

$$<\mathbf{P}^*> \stackrel{\frown}{=} <<\Sigma_2^*>, <\Sigma_3^*>, \ldots>$$

exhibits a one-to-one correspondence between $\mathbf{P}^*$ and $\mathbf{N}$.

Exercise 5.

(i) How many r-plets ($r = 2, \ldots, s$) are there in Σ_s^*?

(ii) What are the 32nd, 33rd and 40th r-plets in $\mathbf{P}^*$?

(iii) From the fact that $\mathbf{P}^*$ is denumerable, deduce that:

(a) $\mathbf{N}\times\mathbf{N}\times\ldots\times\mathbf{N}$ (r factors) $\stackrel{\frown}{=}$ {r-plets of counting numbers}

and

(b) $\mathbf{Q}\times\mathbf{Q}\times\ldots\times\mathbf{Q}$ (r factors) $\stackrel{\frown}{=}$ {r-plets of rationals} are each denumerable for $r = 1, 2, 3, \ldots$.

The full significance of the statement $\mathbf{P}^* \simeq \mathbf{N}$ is best realised in geometric terms. The counting numbers correspond to the 'lattice points' (points with integer co-ordinates) on a 'half-line' (or 'ray') excluding the origin (end point of the half-line), the duplets of counting numbers to lattice points in a quadrant of the plane (excluding the axes), the triplets to the lattice points in an octant of three-dimensional space, and so on. The points of each of these lattices, being elements of denumerable sets, can be put into one-to-one correspondence with the lattice points on a half-line.

But in the geometrical sense we can do better than this. We use an arrangement $<a_1, a_2, \ldots>$ of the rationals $\mathbf{Q}$ (e.g., as obtained in Exercise 4 (ii) in §9.7) to convert the counting numbers in the r-plets into rational numbers, namely, in every r-plet, replace each element $k \in \mathbf{N}$ by $a_k \in \mathbf{Q}$. The correspondence which we established above for the lattices now provides one-to-one correspondences between:

the set $\mathbf{N}$ and the set of points at rational 'distances' from an origin on a line, and the set of points with rational co-ordinates in a plane, and

the set of points with rational co-ordinates in space of three or any number of dimensions.

If we regard physical observations as being concerned only with counting or measuring, then the geometrical system of three spatial dimensions and one temporal dimension in which points have rational co-ordinates provides a complete model for physical space, and in this sense therefore the set N would also provide a complete model for all practical physics! (Shades of Pythagoras!)

Chapter 10

NON-FINITE SETS—NON-DENUMERABLE SETS

In Chapter 9 we showed that various extensions of the set N of counting numbers are nevertheless denumerable sets. It is our aim in this chapter to show that a familiar non-finite set of numbers is not denumerable. We lead up to this result by investigating extensions of the set of rationals obtained by utilising algebraic equations, and eventually discuss the set of algebraic numbers. Finally we examine the set of real numbers.

10.1 *The set $\mathcal{Q}$ of quadratic surds*

It is easily seen that the set whose elements consist of rationals or square roots of positive rationals is denumerable. For we take some arrangement $<a_1, a_2, \ldots>$ of the positive rationals and form the arrangement

$$<0, a_1, -a_1, +\sqrt{a_1}, -\sqrt{a_1}, a_2, -a_2, +\sqrt{a_2}, -\sqrt{a_2}\ldots>.$$

However, by a modification of a previous argument, we can show that the set of 'quadratic surds' is denumerable.

By a quadratic surd we shall mean a quantity

$$\frac{1}{k}(l+m\sqrt{n})$$

where $k \in \mathrm{N}$, $n \in \mathrm{N}$, $l \in \mathbf{I}$, $m \in \mathbf{I}$. This is the most general form of such a quantity, since the more general-looking form,

$\dfrac{p}{p'}+\dfrac{q}{q'}\sqrt{\left(\dfrac{r}{r'}\right)}$, where $p', q', r', r \in \mathrm{N}$, $p, q \in \mathbf{I}$ can be reduced to it by multiplying through by $p'q'r'$ to give

$$\frac{1}{p'q'r'}(pq'r'+p'q\sqrt{rr'}).$$

The quantities $\dfrac{1}{k}(l+m\sqrt{n}), \dfrac{1}{k}(l-m\sqrt{n})$ are the roots of the equation

$$k^2-2klx+l^2-m^2n = 0,$$

which we may write as

$$(kx-l)^2-h = 0,$$

where $k, h \in \mathbf{N}$, $l \in \mathbf{I}$. Thus, if we can arrange the triplets (k, l, h) in order, and then replace each of these by the two roots of the equation in order of magnitude, we shall have put the quadratic surds into one-to-one correspondence with **N**.

Construct first the sets of triplets (k, l, h) of counting numbers with constant sum, thus:

$\Sigma_3 \simeq \{(1, 1, 1)\}$.
$\Sigma_4 \simeq \{(1, 1, 2), (1, 2, 1), (2, 1, 1)\}$.
$\Sigma_5 \simeq \{(1, 1, 3), (1, 2, 2), (1, 3, 1), (2, 1, 2), (2, 2, 1), (3, 1, 1)\}\ldots$

Since $l \in \mathbf{I}$ and $k, h \in \mathbf{N}$, we have to augment the system in such a way as to include the integers and not only the counting numbers as candidates for the middle place. There are two types of additions required: (i) the insertion of a triplet $(k, -l, h)$ beside each triplet (k, l, h) in the list above, so that for example, Σ_4 is replaced by $\Sigma_4^{\pm}$, $\Sigma_4^{\pm} \simeq \{(1, 1, 2), (1, -1, 2), (1, 2, 1), (1, -2, 1), (2, 1, 1), (2, -1, 1)\}$, and (ii) by the insertion of the triplets $(k, 0, h)$ among the triplets (k, l, h). To do this we use the table of duplets (counting number pairs), rewritten as

$\Sigma_2^0 \simeq \{(1, 0, 1)\}$.
$\Sigma_3^0 \simeq \{(1, 0, 2), (2, 0, 1)\}$.
$\Sigma_4^0 \simeq \{(1, 0, 3), (2, 0, 2), (3, 0, 1)\}\ldots$

We arrange the sets of triplets as follows:

$$< \Sigma_2^0, \Sigma_3^{\pm}, \Sigma_3^0, \Sigma_4^{\pm}, \Sigma_4^0, \ldots >.,$$

Next we have to have a rule for arranging the triplets within a set. The triplets $(k, 0, h)$ in Σ_r^0 we arrange in the same order as the duplets (k, h). The triplets in $\Sigma_r^{\pm}$ we arrange 'lexicographically', that is, as before, (k, l, h) precedes (k', l', h') if (i) $k<k'$ or (ii) $k = k'$ and $l<l'$. All the triplets are different and have now been put into one-to-one correspondence with **N**.

In fact this is as far as we need go, since every triplet gives a quadratic surd, and every quadratic surd gives at least one triplet, so that by removing the redundant triplets, we shall obtain an explicit correspondence

$$\mathcal{Q} \simeq \mathbf{N}.$$

It is of interest to investigate which of the triplets are in fact redundant. There are two classes:

(i) If $(k', l', h') = (rk, rl, r^2h)$ where $r \in \mathrm{N}$, then for $r>1$, (k', l', h') is redundant.

(ii) So long as h is not a square, when the triplets (i) have been removed, no two quadratic forms

$$(kx-l)^2-h$$

have a common root, i.e., no two quantities $(l \pm \sqrt{h})/k$ are equal. But if $h = g^2$, where $g \in \mathrm{N}$, then the quadratic surds corresponding to (k, l, g^2) are in fact the rationals $(l \pm g)/k$. If then x is the rational given by $ax+b = 0$, it appears as one of the 'quadratic surds' derived from any quadratic form of the set $\{(ax+b)(cx+d) : a, b$ fixed, $c \in \mathrm{N}, d \in \mathrm{I}\}$. Thus the triplets produce the set $\{(r,s)\}$ of pairs of rationals, as well as the 'genuine' quadratic surds once each.

The first few members of the sequence are:

Triplet (k, l, h)	Quadratic form $(kx-l)^2-h$	Quadratic surds $(l \pm \sqrt{h})/k$
$(1, 0, 1)$	x^2-1	$1, -1$
$(1, 1, 1)$	$(x-1)^2-1$	$2, 0$
$(1, -1, 1)$	$(x+1)^2-1$	0 (omit), -2
$(1, 0, 2)$	x^2-2	$\sqrt{2}, -\sqrt{2}$
$(2, 0, 1)$	$2x^2-1$	$\sqrt{\frac{1}{2}}, -\sqrt{\frac{1}{2}}$
$(1, 1, 2)$	$(x-1)^2-2$	$1+\sqrt{2}, 1-\sqrt{2}$
$(1, -1, 2)$	$(x+1)^2-2$	$-1+\sqrt{2}, -1-\sqrt{2}$
$(1, 2, 1)$	$(x-2)^2-1$	3, 1 (omit)
$(1, -2, 1)$	$(x+2)^2-1$	-1 (omit), -3
– – – –	– – – – –	– – – – – –
$(3, 4, 2)$	$(3x-4)^2-2$	$\frac{1}{3}(4+\sqrt{2}), \frac{1}{3}(4-\sqrt{2})$
– – – –	– – – – –	– – – – – –

Exercise 1. Show that the set of proper quadratic surds (i.e., elements of $\mathcal{Q}$ which are irrational) is denumerable.

10.2 *Polynomials of orders three and greater: algebraic numbers*

Our aim now is to try to extend the results that we obtained for quadratic polynomials and quadratic surds to polynomials of higher degree and 'algebraic numbers'. We consider first the cubic polynomial with rational coefficients (which behaves in somewhat the same way as a quadratic) before exploring further.

The most general cubic polynomial with rational coefficients can be written as

$$f(x) = ax^3+3bx^2+3cx+d,$$

where $\{a, b, c, d\} \subset \mathbf{Q}$ and $a \neq 0$.
If we multiply through by the L.C.M., say k, of the denominators of the coefficients, we obtain the polynomial $kf(x)$ whose coefficients are integers; $f(x) = 0$ and $kf(x) = 0$ have the same roots, so that we may in fact confine our attention to polynomials

$$ax^3+3bx^2+3cx+d$$

in which $a \in \mathrm{N}$ and $\{b, c, d\} \subset \mathbf{I}$.

Since we have assumed $a \neq 0$, that is, that the polynomial is genuinely cubic,

$$ax^3+3bx^2+3cx+d = \frac{1}{a^2}[(ax+b)^3+3\mathrm{H}(ax+b)+\mathrm{G}],$$

where $\mathrm{H} = ac-b^2$, $\mathrm{G} = a^2d-3abc+2b^3$.

A general symbolic solution of the cubic equation was found by Ferro and by Tartaglia, and published in 1545 by Cardan; in modern notation, their solutions of

$$y^3+3\mathrm{H}y+\mathrm{G} = 0$$

are $\quad y = \mathrm{Q}^{1/3}+\kappa\mathrm{Q}^{2/3},\ \omega\mathrm{Q}^{1/3}+\kappa(\omega\mathrm{Q}^{1/3})^2,\ \omega^2\mathrm{Q}^{1/3}+\kappa(\omega^2\mathrm{Q}^{1/3})^2,$

where $\quad \mathrm{Q}^2+\mathrm{GQ}-\mathrm{H}^3 = 0,$

$$\kappa = -\mathrm{H}/\mathrm{Q},$$

and $\quad \omega^2+\omega+1 = 0.$

One at least of the three roots is real, and, if more than one, then all three (unfortunately, Q is complex when all three roots are real). In either case, unless a root is rational, it is the root of only one equation of this standard form.

Exercise 2. Solve completely:

(i) $x^3-2x-4 = 0$ (use $(1+\frac{1}{3}\sqrt{3})^3 = 2+\frac{10}{9}\sqrt{3}$).

(ii) $x^3-7x+6 = 0$.

(These roots can be found at sight, but find Q, show that $2 = \mathrm{Q}^{1/3}+\kappa\mathrm{Q}^{2/3}$, and check that the formulae do actually give the roots.)

(iii) $x^3+x+1 = 0$.

(Solve this formally, giving the root as $\mathrm{Q}^{1/3}+\kappa\mathrm{Q}^{2/3}$ without trying to reduce $\mathrm{Q}^{1/3}$. Then solve the equation approximately numerically and compare the value obtained with the value of $\mathrm{Q}^{1/3}+\kappa\mathrm{Q}^{2/3}$.)

The next step on the way to algebraic numbers is the quartic polynomial and the roots of quartic equations

$$a_0x^4+a_1x^3+a_2x^2+a_3x+a_4 = 0,$$

in which $a_0 \in \mathrm{N}$, $a_r \in \mathbf{I}$, $(r = 1, 2, 3, 4)$ and the five numbers a_i have no common factor. Again a formal solution of very long standing exists to this type of equation (Ferrari, a pupil of Cardan); there may be four solutions, or two solutions, or no solutions in real numbers.

For quadratic, cubic and quartic equations we have the formal algebraic methods outlined above for finding solutions of particular equations. At the step from equations of degree 4 to equations of degree 5 there is a significant change: Abel proved in 1821 that there does not exist a formal solution to the general equation of degree 5. That is, if we write this general equation as

$$a_0x^5+a_1x^4+a_2x^3+a_3x^2+a_4x+a_5 = 0,$$

where $a_0 \in \mathrm{N}$, $a_r \in \mathrm{I}$ $(r = 1, 2, 3, 4, 5)$, then it is impossible to give a formula expressing the roots of this equation in terms of the coefficients $a_0, \ldots, a_5$. Therefore, we must clearly understand the meaning of a phrase such as 'the solution of a given equation of degree 5'. [In fact, it is known that it is impossible to give a formal solution of the general equation of any degree greater than 4, so that the equations of small degree are really exceptions to the general rule.]

Firstly, the 'fundamental theorem of algebra', in the form in which we need it, is

'Any algebraic equation in which the coefficients are integers has at least one solution in the field of complex numbers'. That is, given any polynomial

$$f(x) = a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n,$$

in which $n \in \mathrm{N}$, $a_0 \in \mathrm{N}$, $a_i \in \mathbf{I}$ $(r = 1, \ldots, n)$, then there is a complex number z for which

$$f(z) = a_0z^n+a_1z^{n-1}+\ldots+a_{n-1}z+a_n = 0,$$

i.e., z is a root of the equation $f(x) = 0$.

When this is accepted, it is easy to prove that a function

$$\sum_{i=0}^{n} a_ix^{n-i}$$

can be written as a_0 times the product of n factors $x+q$ where q is in the field of complex numbers, and that the factors in which q is actually complex occur in conjugate pairs (so that, if n is odd, at least one of the numbers q is real).

The second statement is the one above, namely, that for $n \geq 5$, the equation

$$f(x) = \sum_{i=0}^{n} a_i x^{n-i} = 0$$

has no formal solution, corresponding to those for the quadratic, cubic and quartic equations.

The third statement is that we can find a rational number which differs from the number which is a real solution to $f(x) = 0$ by less than any assigned rational number. (A corresponding statement is true for complex solutions.) An approximate solution of this sort is obtained as the result of drawing a graph or of an iterative process such as Newton's or Horner's or of a programme for an electronic computer.

The set of solutions to equations of the form

$$\sum_{i=0}^{n} a_i x^{n-i} = 0$$

where $a_0 \in \mathbf{N}$, $a_r \in \mathbf{I}$ $(r = 1, 2, \ldots, n)$, $n \in \mathbf{N}$, is the set A of algebraic numbers. From what has been said above, it will be realised that in general an algebraic number is defined only by an equation of which it is a root, and not (as in the case of a cubic) by an explicit expression such as $\mathrm{Q}^{1/3} + \kappa \mathrm{Q}^{2/3}$. An approximation to any algebraic number can be found by some iterative method of solving an equation which it satisfies. The set of real algebraic numbers (in general, solutions of algebraic equations are complex numbers) is denoted by **A**.

Exercise 3. An algebraic number a is algebraic of degree $n > 0$ if it satisfies an equation

$$\sum_{i=0}^{n} a_i x^{n-i} = 0 \qquad (a_0 \in \mathbf{N}, a_r \in \mathbf{I}\ (r = 1, \ldots, n)),$$

but satisfies no equation with rational coefficients of degree 1 or 2 or ... or $n-1$. By considering the equations $x^n - p = 0$ $(n \in \mathbf{N}$, $p \in \mathbf{N}$ and is a prime) show that, for each $n \in \mathbf{N}$, the set $\mathbf{A}(n)$ of real algebraic numbers of degree n is non-finite.

10.3 *The sets A and* **A**

Since $\mathbf{A} \subset A$, we can show that **A** is denumerable by proving the denumerability of A. The idea of the proof is as follows. An algebraic number is a root of an algebraic equation with integer coefficients.

If we can show that the set of such equations is denumerable, then, since an equation of degree n has at most n distinct roots, A is denumerable.

Let P be the set of polynomials $p(x)$ of the form:

$$p(x) \equiv x, \text{ or}$$
$$p(x) \equiv a_0x^n + a_1x^{n-1} + \ldots + a_n,$$

where $n \in \mathrm{N}$, $a_0 \in \mathrm{N}$, $a_r \in \mathrm{I}$ $(r = 1, 2, \ldots, n-1)$ and $a_n \in \mathrm{I} - \{0\}$.

[Thus the coefficient of the highest power of x is a counting number, the constant term is a non-zero integer, and the other coefficients are integers.]

If we wish to count the elements of P, we must devise a way of arranging them in order so that each polynomial $p(x) \in P$ appears at least once and preferably once only. There are two measures of 'size' that suggest themselves: the size of the coefficients of $p(x)$, and the degree of $p(x)$. We examine these first:

(a) If we use the magnitude of the largest coefficient in $p(x)$ as a measure of size, then clearly each of the polynomials

$$x+1,\ x^2+x+1,\ x^3+x^2+x+1,\ \ldots$$

has size 1, and they form a non-finite set.

(b) If we use the sum of the magnitudes of the coefficients of $p(x)$ as a measure of size, we are no further, since each of the polynomials

$$x+1,\ x^2+1,\ x^3+1,\ \ldots$$

has size 2, and they form a non-finite set.

(c) If we use the degree n of $p(x)$ as a measure of size, then each of

$$x^2+1,\ x^2+2,\ x^2+3,\ \ldots$$

has size 2, and these polynomials again form a non-finite set.

Each of the methods (a), (b), (c) yields a non-finite set of polynomials having given size and so we must devise, for each such set, a way of counting its elements. Even when that is done, we have then to show that a denumerable collection of denumerable sets (for we have one such set for each size 1, 2, 3, ...) forms a set which is denumerable. Only when this has been achieved will we have accomplished our task. Instead, let us try to devise a measure of size which produces, for each size, a finite subset of P, and not a non-finite subset. The examples (a), (b), (c) indicate that such a measure must restrict both the magnitude of the coefficients of a polynomial and its degree. We are led to introduce a measure of size which is a combination of (b) and (c) above.

The **height**, $h(p)$, of p is the counting number

$$h(p) = n+a_0+|a_1|+\ldots+|a_n|,$$

where $$|a_i| = a_i \text{ if } a_i \geq 0, \quad |a_i| = -a_i \text{ if } a_i < 0.$$

Exercise 4. Show that there are only finitely many elements $p(x)$ of P which have a given height h.

For each $h \in \mathrm{N}$, let $P(h) \doteq \{\text{all elements of } P \text{ of height } h\}$.
For example,

$P(1) \doteq \varnothing$,
$P(2) \doteq \{x\}$,
$P(3) \doteq \{x-1, x+1\}$,
$P(4) \doteq \{x^2+1, x^2-1, 2x+1, 2x-1, x+2, x-2\}$,
$P(5) \doteq \{x^3+1, x^3-1, 2x^2-1, 2x^2+1, x^2+x+1, x^2-2, x^2+2, x^2+x-1, x^2-x+1, x^2-x-1, 3x-1, 3x+1, 2x-2, 2x+2, x+3, x-3\}$.

Each $p \in P$ belongs to precisely one subset $P(h)$, namely the subset $P(h(p))$. We arrange these subsets in the order $<P(2), P(3), P(4), \ldots>$. Then, if we specify an arrangement of $P(h)$ for each h, we have an arrangement of P.

To do this, we follow the arrangement of $\mathbf{P}^*$ previously obtained. Associate with the element $p(x) \in P(h)$ the $(n+2)$-plet $(n, a_0, a_1, \ldots, a_n)$, where n is the degree of $p(x)$. Then $p(x) = a_0x^n+a_1x^{n-1}+\ldots+a_n$, of height h, precedes $q(x) = b_0x^m+b_1x^{m-1}+\ldots+b_m$, of height h, if $n<m$ or (if $n = m$) if the first non-zero difference $a_0-b_0, a_1-b_1, \ldots, a_n-b_n$ is negative. Denote by $<P(h)>$ the arrangement of $P(h)$ thus obtained.

For example,

$<P(2)> \doteq <x>$,
$<P(3)> \doteq <x-1, x+1>$,
$<P(4)> \doteq <x-2, x+2, 2x-1, 2x+1, x^2-1, x^2+1>$
$<P(5)> \doteq <x-3, x+3, 2x-2, 2x+2, 3x-1, 3x+1, x^2-x-1, x^2-x+1, x^2-2, x^2+2, x^2+x-1, x^2+x+1, 2x^2-1, 2x^2+1, x^3-1, x^3+1>$.

Then, $$<P> \doteq <<P(2)>, <P(3)>, \ldots>$$

is an arrangement of P giving a one-to-one correspondence of P with N.

In order to proceed from P to A, we observe that:

(i) different elements $p(x)$, $q(x)$ of P may yield the same element of A. This happens in two ways: (a) if for some $k \in \mathrm{N}$, $k \neq 1$, $p(x) \equiv kq(x)$, then the roots of $q(x) = 0$ are the roots of $p(x) = 0$; (b) if for some $f(x) \in P$, $p(x) \equiv f(x)q(x)$, then the roots of $p(x) = 0$ include the roots of $q(x) = 0$.

(ii) An element $p(x)$ of P, of degree n, may produce as many as n distinct elements of A.

Therefore, we lay down the following rules.

1. In the given arrangement $<P>$ of P, delete those elements $p(x)$ of the forms

$$p(x) \equiv kq(x),\ k \neq 1,\ k \in \mathrm{N},\ q(x) \in P,$$
$$p(x) \equiv f(x)q(x),\ f(x) \in P,\ q(x) \in P.$$

The elements remaining in P form a denumerable subset P' of P. Denote by $<P'>$ the arrangement of P' derived from $<P>$.

For example, the subsets $P'(h)$ of elements of P' of height h are arranged as

$$\begin{aligned} <P'(2)> &\doteq <x>,\\ <P'(3)> &\doteq <x-1,\ x+1>,\\ <P'(4)> &\doteq <x-2,\ x+2,\ 2x-1,\ 2x+1,\ x^2+1>,\\ <P'(5)> &\doteq <x-3,\ x+3,\ 3x-1,\ 3x+1,\ x^2-x-1,\ x^2-x+1,\\ &\qquad x^2-2,\ x^2+2,\ x^2+x-1,\ x^2+x+1,\ 2x^2-1,\\ &\qquad 2x^2+1>. \end{aligned}$$

2. [It can be proved, using properties of **I**, that no two elements of P' have a common root and that no element of P' has a repeated root, but we shall not assume these facts.] Let $p(x)$ be an element of P' of degree n, with roots $p_1, \ldots, p_n$ which will in general be complex numbers $p_j = x_j + iy_j$ with x_j, y_j real. If $p_j (j = 1, 2, \ldots, n)$ is a root of $q(x) = 0$, where $q(x)$ precedes $p(x)$ in $<P'>$, delete it. If $p_j = p_k$ for some $k<j$, delete p_j. Arrange the remaining roots $p_1, \ldots, p_r$ (there may be none) by the rule p_k precedes p_l if the first of the non-zero differences $x_k - x_l$, $y_k - y_l$ is negative, giving the arrangement $<p_1, \ldots, p_r>$. Then A can be arranged as follows: replace each element $p(x)$ of $<P'>$ by the above arrangement $<p_1, \ldots, p_r>$. Clearly, each algebraic number appears once and once only, so we have a one-to-one correspondence of A with **N**. **A**, as a subset of A, is thus denumerable, and we in fact have an arrangement of **A** directly if we replace rule 2 above by rule 2.1:

2.1 Let $p(x)$ be an element of P' of degree n, and let $p_1, \ldots, p_m$

$(m \leq n, m \in \mathrm{N})$ be the real roots of $p(x) = 0$. Delete p_j $(j = 1, 2, \ldots, m)$ if it is a root of $q(x) = 0$, where $q(x)$ precedes $p(x)$ in $<P'>$. If $p_j = p_k$ for some $k<j$, then delete it. Arrange the remaining roots $p_1, \ldots, p_r$ (there may be none) by the rule p_k precedes p_l if $p_k - p_l$ is negative.

The first few numbers $\alpha_1, \alpha_2, \ldots$ of $<\mathrm{A}>$ according to this arrangement are shown in the following table.

r-plet $(n, a_0, \ldots, a_n)$	$p(x)$	roots $p_1, \ldots p_n$	α_i
$(1, 1)$	x	0	$\alpha_1 = 0$
$(1, 1, -1)$	$x-1$	1	$\alpha_2 = 1$
$(1, 1, 1)$	$x+1$	-1	$\alpha_3 = -1$
$(1, 1, -2)$	$x-2$	2	$\alpha_4 = 2$
$(1, 1, 2)$	$x+2$	-2	$\alpha_5 = -2$
$(1, 2, -1)$	$2x-1$	$\frac{1}{2}$	$\alpha_6 = \frac{1}{2}$
$(1, 2, 1)$	$2x+1$	$-\frac{1}{2}$	$\alpha_7 = -\frac{1}{2}$
$(2, 1, 0, 1)$	x^2+1	no real root	
$(1, 1, -3)$	$x-3$	3	$\alpha_8 = 3$
$(1, 1, 3)$	$x+3$	-3	$\alpha_9 = -3$
$(1, 3, -1)$	$3x-1$	$\frac{1}{3}$	$\alpha_{10} = \frac{1}{3}$
$(1, 3, 1)$	$3x+1$	$-\frac{1}{3}$	$\alpha_{11} = -\frac{1}{3}$
$(2, 1, -1, -1)$	x^2-x-1	$\dfrac{1 \pm \sqrt{5}}{2}$	$\alpha_{12} = \dfrac{1-\sqrt{5}}{2} \doteqdot -0.618033$
			$\alpha_{13} = \dfrac{1+\sqrt{5}}{2} \doteqdot 1.618033$
$(2, 1, 0, -2)$	x^2-2	$\pm\sqrt{2}$	$\alpha_{14} = -\sqrt{2} \doteqdot -1.4142135$ $\alpha_{15} = +\sqrt{2} = -\alpha_{14}$
$(2, 1, 0, 2)$	x^2+2	no real root	
$(2, 1, 1, -1)$	x^2+x-1	$\dfrac{-1 \pm \sqrt{5}}{2}$	$\alpha_{16} = -\alpha_{13}$
			$\alpha_{17} = -\alpha_{12}$
$(2, 2, 0, -1)$	$2x^2-1$	$\pm \dfrac{1}{\sqrt{2}}$	$\alpha_{18} = \dfrac{-1}{\sqrt{2}} = \frac{1}{2}\alpha_{14}$ $= -0.7071067$
			$\alpha_{19} = \dfrac{1}{\sqrt{2}} = \frac{1}{2}\alpha_{15}$ $= 0.7071067$
$(2, 2, 0, 1)$	$2x^2+1$	no real root	

10.4 *The set* **R** *of real numbers: the continuum*

The last question to be asked (and historically the last to be answered) is: 'Is there any real number which is not a real algebraic number, i.e., not a root of a polynomial equation with integer coefficients?' The answer is 'yes', and was first given by Liouville in 1844 by showing how to construct real numbers (defined as the limiting sums of convergent infinite series of a certain type) which could be shown to be non-algebraic. Such numbers (real or complex) are called transcendental numbers. We shall use a different method (used first by Cantor) to demonstrate the existence of transcendental numbers. As we shall see, Cantor's method does not produce explicit transcendental numbers, and in fact the problem of determining whether or not a given real number (defined by some limiting process) is transcendental is usually very difficult. For example,

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = \sum_{r=0}^{\infty}\frac{1}{r!}$$

was shown to be transcendental by Hermite in 1873,

$$\pi = 1-\tfrac{1}{3}+\tfrac{1}{5}-\tfrac{1}{7}+\ldots$$

was proved transcendental by Lindemann in 1882, while it is still not known whether Euler's constant

$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log_e n\right)$$

is rational, algebraic, or transcendental.

We have given in §10.3 an arrangement <A> of the real algebraic numbers. By deleting all numbers of A which do not lie in the interval $0 \leq x \leq 1$, we are left with an arrangement, <A'>, say, of the algebraic numbers between 0 and 1 (inclusive).

Using our table, the first few numbers are:

$$\begin{aligned}
\alpha_1' &= \alpha_1 = 0 && = 0.000\ 000\ \ldots\\
\alpha_2' &= \alpha_2 = 1 && = 1.000\ 000\ \ldots\\
\alpha_3' &= \alpha_6 = \tfrac{1}{2} && = 0.500\ 000\ \ldots\\
\alpha_4' &= \alpha_{10} = \tfrac{1}{3} && = 0.333\ 333\ \ldots\\
\alpha_5' &= \alpha_{13} = \frac{\sqrt{5}-1}{2} && = 0.618\ 033\ \ldots\\
\alpha_6' &= \alpha_{19} = \frac{\sqrt{2}}{2} && = 0.707\ 106\ \ldots.
\end{aligned}$$

Now construct the number

$$x = 0.x_1x_2x_3 \ldots$$

by the rule that for each $i \in \mathrm{N}$,

$x_i = 3$ if the i-th decimal digit of α_i' is not 3,
$x_i = 0$ if the i-th decimal digit of α_1' is 3.

Thus $x = 0.333003 \ldots$. Then $x \neq \alpha_i'$ for any $i \in \mathrm{N}$, since x differs from α_i' in the i-th decimal place.

It should be noted that in constructing x we could have selected any one of nine choices for each digit x_i. But equally we could have constructed a number $b = 0.b_1b_2b_3b_4b_5b_6 \ldots$, where

b_1 is different from the first digit of α_1',
b_2b_3 are different from the second and third digits of α_2',
$b_4b_5b_6$ are different from the fourth, fifth and sixth digits of α_3', etc.

That is, in constructing b, α_1' gave nine choices, α_2' gave 99 choices, α_3' gave 999 choices ....

The inference to be made is that there are 'many more' transcendental numbers than there are algebraic numbers, but, remembering that in the same sense, there are 'many more' algebraic numbers than counting numbers, we cannot infer that it is not possible to establish a one-to-one correspondence between the set **R** of numbers expressible in the decimal notation (that is, the algebraic numbers together with the transcendentals) and the counting numbers.

We have however in **R** arrived at last at a set which is not in one-to-one correspondence with the counting numbers. For consider the subset **R**$'$ of members x of **R** in the range $0<x<1$, and suppose that we have devised a rule which establishes the following one-to-one correspondence between N and **R**$'$:

N	**R**$'$
1	$0.\,a_1a_2a_3a_4 \ldots$
2	$0.\,b_1b_2b_3b_4 \ldots$
3	$0.\,c_1c_2c_3c_4 \ldots$
4	$0.\,d_1d_2d_3d_4 \ldots.$

As we did before, form a number

$$q = 0.\,a_1'b_2'c_3'd_4' \ldots$$

in which, for each m, the m-th digit is different from the m-th digit in the m-th number of the sequence above. Then q cannot belong to the sequence above, because it differs in at least one decimal digit from any number in that sequence. That is, we have found a number in the range (0, 1) which does not belong to the sequence which we assumed to contain every member in the range (0, 1). This is a contradiction. It is therefore not possible to establish a one-to-one correspondence between **N** and **R**′, and therefore *a fortiori* not between **N** and **R**.

Having found that **N** can be put into one-to-one correspondence with $\mathbf{N}\times\mathbf{N}$, we are led to investigate the possibility of establishing a correspondence between **R** and $\mathbf{R}\times\mathbf{R}$. Surprisingly, this is relatively simple to do: we have to specify a correspondence

$$(x, y)\leftrightarrow X, \quad x, y, X\in\mathbf{R}.$$

We shall have achieved sufficient of our purpose if we specify it for X in the domain $0<X<1$ and (x, y) in $0<x<1$, $0<y<1$. A one-to-one correspondence is established by taking for each pair (x, y), where

$$x = 0.r_1r_2r_3 \dots$$
$$y = 0.s_1s_2s_3 \dots,$$

the corresponding X to be

$$X = 0.r_1s_1r_2s_2r_3s_3 \dots .$$

In geometric language this is a one-to-one correspondence between the points of a unit interval on a line and the points of a unit square in a plane, a correspondence which was a stumbling block in the path of mathematical philosophers for some years at the beginning of this century, because of their deep-seated feeling that it was impossible that a 'line' and a 'plane' could provide two interpretations of the same geometric system, that is, in general terms, that its 'dimension' was a fundamental invariant of a space. The difficulty was resolved by Brouwer in 1911 when he proved that there could be no one-to-one correspondence between points of a line and points of a plane in which every pair of points which were 'close together' on the line corresponded to a pair of points which were 'close together' in the plane. In other words, 'dimension' is invariant under continuous transformations.

Another question which suggests itself is: is it possible to specify sets which cannot be put into one-to-one correspondence with **R**? The answer is 'yes', and the proof of their existence depends on a theorem to the effect that the set of subsets of a non-empty set S cannot be put into one-to-one correspondence with any subset of S.

For finite sets this is trivial, since, if the number of elements in S is n, the number of subsets is 2^n (and, in any case, one subset of the set of subsets is the set of subsets each consisting of a single member of S!). The reader will realise however that for non-finite sets the theorem is anything but trivial.

The next phase of the investigation of the properties of sets might begin with the consideration of such sets as

$$G \triangleq \{1+(\tfrac{1}{2})^n : n \in N\},$$

and

$$H \triangleq \{2m-1+(\tfrac{1}{2})^n : m, n \in N\},$$

both of which are clearly denumerable. As the definitions stand, $1 \notin G$ and no member of the set of odd counting numbers belongs to H; these are gaps in the sets which can cause considerable inconvenience in framing theorems and proofs. We can fill the gaps by replacing G and H by

$$G^* \triangleq \{1\} \cup G,$$

and

$$H^* \triangleq \{2m-1,\ m \in N\} \cup H,$$

operations which are simple enough in these cases, but could clearly bristle with difficulties in the sort of pathological case which tends to invalidate the more optimistically conceived type of theorem.

Beyond this point in fact the problems posed by the structure of sets are no longer problems associated primarily with the simple sorting process, rather they are those associated with the more sophisticated concept of limits; such problems are beyond the scope of this book. The authors' hope is that the reader will have been inspired to continue his study of the Theory of Sets, and plunge into these deeper waters. As guides to the way he might study:

P. R. Halmos: *Naive Set Theory*,
R. R. Stoll: *Set Theory and Logic*,
A. A. Fraenkel: *Abstract Set Theory*,

in all of which abundant references for further reading will be found.

APPENDIX

Solutions to and comments on some of the exercises.

Chapter 2

Exercise 1. $A \cap B \cap C \bumpeq (A \cap B) \cap C$

$$\bumpeq A \cap (B \cap C). \text{ (insertion of parentheses)}$$

Since $A \cap B \bumpeq B \cap A$, etc., we have

$$A \cap B \cap C \bumpeq (B \cap A) \cap C$$
$$\bumpeq A \cap (C \cap B).$$

Since also $(A \cap B) \cap C \bumpeq C \cap (A \cap B)$ etc., we have

$$A \cap B \cap C \bumpeq C \cap (A \cap B)$$
$$\bumpeq (B \cap C) \cap A,$$

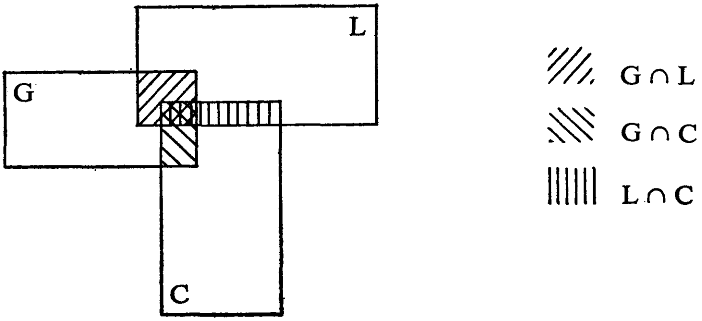
and also

$$A \cap B \cap C \bumpeq C \cap (B \cap A)$$
$$\bumpeq (C \cap B) \cap A.$$

Removing parentheses in the last six expressions (as we may do by the associativity of intersection), we also have:

$$A \cap B \cap C \bumpeq B \cap A \cap C \bumpeq A \cap C \cap B$$
$$\bumpeq C \cap A \cap B \bumpeq B \cap C \cap A$$
$$\bumpeq C \cap B \cap A \bumpeq C \cap B \cap A.$$

Exercise 2.



$$G \cap L \cap C \subset G \cap L$$
$$G \cap L \cap C \subset G \cap C$$
$$G \cap L \cap C \subset L \cap C.$$

It would be incorrect to write the three relations above in a shortened form as

$$\begin{aligned} G \cap L \cap C &\subset G \cap L \\ &\subset G \cap C \\ &\subset L \cap C, \end{aligned}$$

because the meaning of this statement is the same as that of

$$G \cap L \cap C \subset G \cap L \subset G \cap C \subset L \cap C,$$

and clearly $G \cap L \not\subset G \cap C$, $G \cap C \not\subset L \cap C$, $G \cap L \not\subset L \cap C$.
[cf. a similar situation using numbers: $2<5$, $2<3$, and $2<7$, but

$$\begin{aligned} 2 &< 5 \\ &< 3 \\ &< 7 \end{aligned}$$

means $2<5<3<7$, a chain of inequalities which is clearly incorrect, since $5 \not< 3$.]

Exercise 3. (i) $$\begin{aligned} A \cap A &\bumpeq \{k : k \in A \text{ and } k \in A\} \\ &\bumpeq \{k : k \in A\} \\ &\bumpeq A. \end{aligned}$$

(ii) If $k \in A \cap C$, then $k \in A$ and $k \in C$. But, since $A \subseteq B$, if $k \in A$, then we know $k \in B$. Hence $k \in B$ and $k \in C$ so $k \in B \cap C$.

Thus every element of $A \cap C$ is an element of $B \cap C$, i.e.,

$$A \cap C \subseteq B \cap C.$$

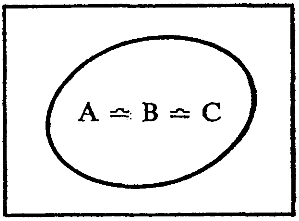
(iii) $A \cap B \bumpeq U$, and so each element of U belongs both to A and to B, for if not, $A \cap B \not\bumpeq U$. Thus each element of U belongs to A, and each element of U belongs to B. Hence $U \subseteq A$ and $U \subseteq B$. But A and B are each subsets of U, so $A \subseteq U$ and $B \subseteq U$. Thus $U \bumpeq A \bumpeq B$.

Exercise 4. The total number of different possible relations among three subsets of a set is quite large, and this is discussed later in the book. We list here some of the possibilities.

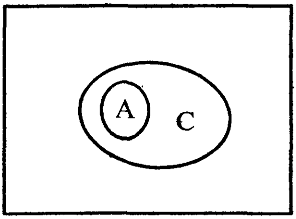
Suppose that each of A, B, C is a proper subset of U, i.e.,

$$\emptyset \subset A \subset U, \ \emptyset \subset B \subset U, \ \emptyset \subset C \subset U.$$

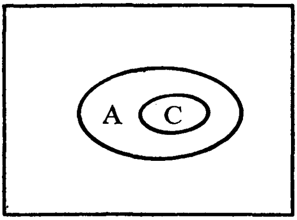
(i) The simplest case is $A \bumpeq B \bumpeq C$, with diagram:



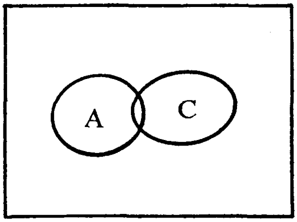
(ii) If, say $A \bumpeq B$, we have the possibilities:



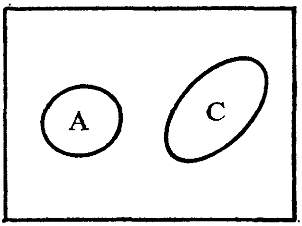
$A \subset C$



$C \subset A$



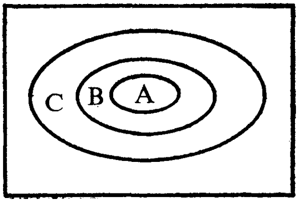
$\varnothing \subset A \cap C \subset A$
$A \cap C \subset C$



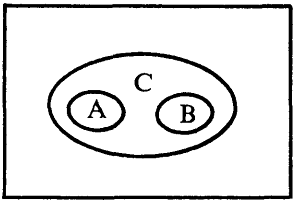
$A \cap C \bumpeq \varnothing$

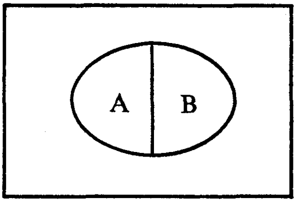
(iii) If A, B, C are all different, there may or may not be an inclusion relation between pairs of them.

(a) If, say, $A \subset B \subset C$, we have:

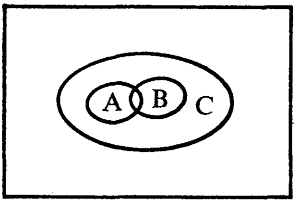


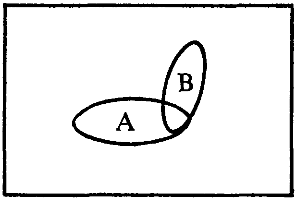
(b) If, say, $A \subset C$, $B \subset C$, we have one of:





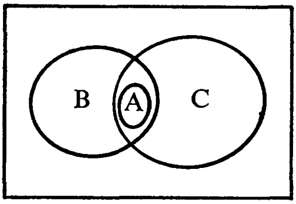
$C \bumpeq A \cup B$



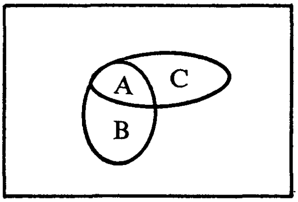


$C \bumpeq A \cup B$

(c) If, say, $A \subset B$, $A \subset C$, we have either:



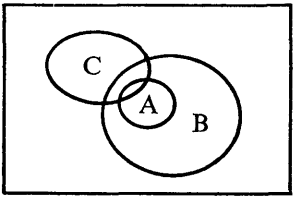
or:

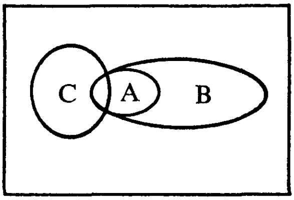


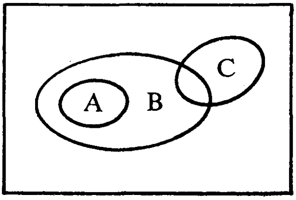
$A \subset B \cap C$

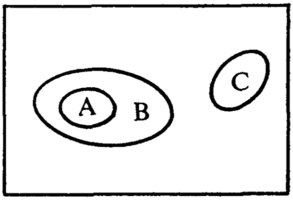
$A \bumpeq B \cap C$

(d) If, say, $A \subset B$ there are the four cases corresponding to diagrams:





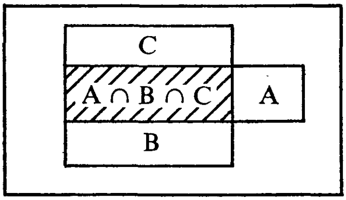




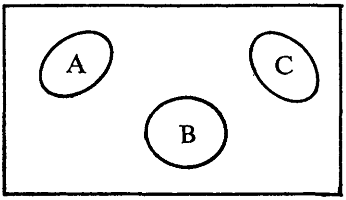
(There is another, in which C fills the whole region not occupied by B.)

(e) When no inclusions hold, diagrams range from that for the case

$$A \cap B \bumpeq B \cap C \bumpeq C \cap A \bumpeq A \cap B \cap C \not\bumpeq \emptyset:$$



to $$A \cap B \bumpeq B \cap C \bumpeq C \cap A \bumpeq \emptyset:$$



Exercise 5. Adding 4 objects to a pile composed of a heap of 3 objects and a heap of 2 objects produces the same number of objects as adding 2 objects to a pile consisting of one heap of 3 and one heap of 4, since in each case we are simply adding together the 3 heaps of objects.

Exercise 6. The associative law for $\cap$ enables us to rearrange the parentheses in $(A \cap B) \cap (C \cap D)$ as follows:

$$\begin{aligned}(A \cap B) \cap (C \cap D) &\bumpeq A \cap (B \cap (C \cap D)) \\ &\bumpeq A \cap ((B \cap C) \cap D),\end{aligned}$$

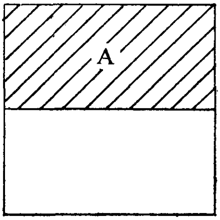
now we may omit the outer parentheses, obtaining

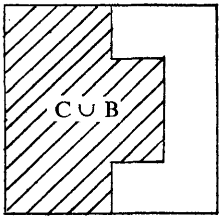
$$(A \cap B) \cap (C \cap D) \bumpeq A \cap (B \cap C) \cap D.$$

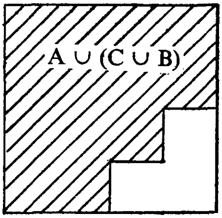
Exercise 9.
$$\begin{aligned}A \cup B \cup C &\bumpeq \{k : k \in A \text{ or } k \in B \text{ or } k \in C\}. \\ A \cup B \cup C &\bumpeq A \cup (B \cup C) \bumpeq (B \cup C) \cup A \\ &\bumpeq A \cup (C \cup B) \bumpeq (C \cup B) \cup A.\end{aligned}$$

Also
$$\begin{aligned} \mathrm{A}\cup\mathrm{B}\cup\mathrm{C} &\bumpeq (\mathrm{A}\cup\mathrm{B})\cup\mathrm{C} \bumpeq \mathrm{C}\cup(\mathrm{A}\cup\mathrm{B}) \\ &\bumpeq (\mathrm{B}\cup\mathrm{A})\cup\mathrm{C} \bumpeq \mathrm{C}\cup(\mathrm{B}\cup\mathrm{A}). \end{aligned}$$

Sample diagram for $\mathrm{A}\cup\mathrm{B}\cup\mathrm{C} \bumpeq \mathrm{A}\cup(\mathrm{C}\cup\mathrm{B})$:







Exercise 10. (i)
$$\begin{aligned} \mathrm{A}\cup\mathrm{A} &\bumpeq \{k : k \in \mathrm{A} \text{ or } k \in \mathrm{A}\} \\ &\bumpeq \{k : k \in \mathrm{A}\} \\ &\bumpeq \mathrm{A}. \end{aligned}$$

(ii) $\mathrm{A}\cup\mathrm{C} \bumpeq \{k : k \in \mathrm{A} \text{ or } k \in \mathrm{C}\}$.

If $k \in \mathrm{A}\cup\mathrm{C}$, and $k \notin \mathrm{C}$, then $k \in \mathrm{A}$. Since $\mathrm{A} \subseteq \mathrm{B}$, $k \in \mathrm{B}$. So if $k \in \mathrm{A}\cup\mathrm{C}$, $k \in \mathrm{B}$ or $k \in \mathrm{C}$, i.e., $k \in \mathrm{B}\cup\mathrm{C}$.

Hence $\mathrm{A}\cup\mathrm{C} \subseteq \mathrm{B}\cup\mathrm{C}$ if $\mathrm{A} \subseteq \mathrm{B}$.

(iii) $\mathrm{A}\cup\mathrm{B}$ consists of all elements in A or B. If it has no elements, then neither A nor B can have elements, i.e.,

$$\mathrm{A} \bumpeq \mathrm{B} \bumpeq \emptyset.$$

Exercise 11. We use the transitivity of '$\subseteq$'. We have seen previously that for all A, B,

$$\mathrm{A}\cap\mathrm{B} \subseteq \mathrm{A} \text{ and } \mathrm{A} \subseteq \mathrm{A}\cup\mathrm{B}.$$

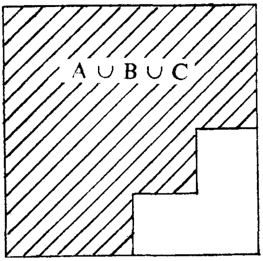
Hence $\qquad \mathrm{A}\cap\mathrm{B} \subseteq \mathrm{A} \subseteq \mathrm{A}\cup\mathrm{B}$,

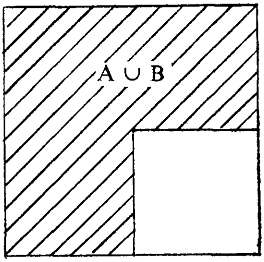
and so $\qquad \mathrm{A}\cap\mathrm{B} \subseteq \mathrm{A}\cup\mathrm{B}$.

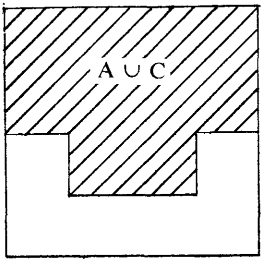
Exercise 12.
$$\begin{aligned} (\mathrm{A}\cup\mathrm{B})\cup(\mathrm{C}\cup\mathrm{D}) &\bumpeq \mathrm{A}\cup(\mathrm{B}\cup(\mathrm{C}\cup\mathrm{D})) \\ &\bumpeq \mathrm{A}\cup((\mathrm{B}\cup\mathrm{C})\cup\mathrm{D}) \\ &\bumpeq \mathrm{A}\cup(\mathrm{B}\cup\mathrm{C})\cup\mathrm{D}. \end{aligned}$$

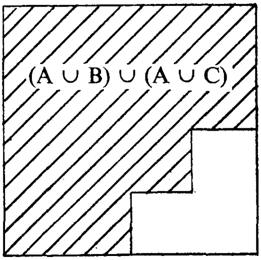
The first two steps used the associative law directly. The last step used the associate law to justify the removal of one set of parentheses.

Exercise 13.









$$\begin{aligned}(A \cup B) \cup (A \cup C) &\bumpeq A \cup (B \cup A) \cup C && \text{(by Ex. 12 above)}\\ &\bumpeq A \cup (A \cup B) \cup C && \text{(commutative law)}\\ &\bumpeq (A \cup A) \cup B \cup C && \text{(associative law)}\\ &\bumpeq A \cup B \cup C. && \text{(by Ex. 10 (i) above)}\end{aligned}$$

The other proof is similar.

Exercise 14. (i) The elements not belonging to G are the elements of B($\bumpeq \tilde{G}$). The elements not belonging to the subset of elements not belonging to G are thus the elements not belonging to the subset B. Hence the required subset is $\tilde{B} \bumpeq G$. The result $\tilde{\tilde{A}} \bumpeq A$ is an example of a 'double negative'. Compare the sentences:

It is true that I was at the beach today.
It is true that I was not at the beach today.
It is not true that I was not at the beach today.

(ii)
$$\begin{aligned}A \cup \tilde{A} &\bumpeq \{\text{all elements of U in A}\} \cup \{\text{all elements of U not in A}\}\\ &\bumpeq \{\text{all elements of U}\}\\ &\bumpeq U.\\ A \cap \tilde{A} &\bumpeq \{x : x \in U,\ x \in A \text{ and } x \in \tilde{A}\}\\ &\bumpeq \{x : x \in U,\ x \in A \text{ and } x \notin A\}\\ &\bumpeq \emptyset, \text{ since no element } x \text{ can simultaneously belong}\end{aligned}$$

to A and not belong to A. Each of U, $\emptyset$ is independent of the subset A.

(iii) If $A \subseteq B$, we know $A \cap \tilde{B} \subseteq B \cap \tilde{B} \bumpeq \emptyset$, so $A \cap \tilde{B} \bumpeq \emptyset$. Also $U \bumpeq \tilde{A} \cup A \subseteq \tilde{A} \cup B \subseteq U$, whence $\tilde{A} \cup B \bumpeq U$.

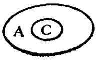
Exercise 16. (i) The required subset is $B \cap (L \cup S)$.

(ii) $\cup$ is a commutative operation, so

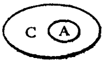
$$B \cup C \bumpeq C \cup B.$$

Hence $$A \cap (B \cup C) \bumpeq A \cap (C \cup B).$$

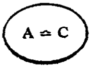
(iii) (a) When $B \subset C$, $B \cup C \bumpeq C$, and $A \cap (B \cup C) \bumpeq A \cap C$. The possibilities:



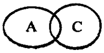
(i)



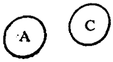
(ii)



(iii)



(iv)



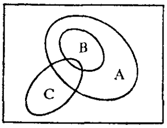
(v)

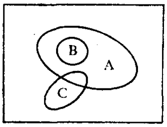
may occur.

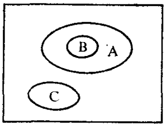
Examples of each drawn from the class:

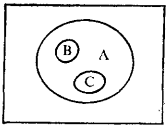
(i) $V \subset G \subset \tilde{S}$,
(ii) $S \subset C$, $B \subset C$,
(iii) $L \cap G \subset L$, $L \bumpeq P$,
(iv) $S \subset B$, $B \cap L \not\bumpeq \emptyset$,
(v) $V \subset G$, $G \cap S \bumpeq \emptyset$.

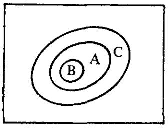
(b) When $B \subset A$, $A \cap (B \cup C) \bumpeq B \cup (A \cap C)$. The following situations may occur:

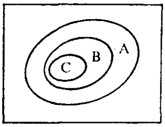


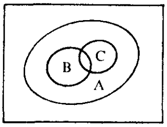












Exercise 21. 'Children who are both girls or left-handed and girls or have a name beginning with a consonant' describes the same children as 'Children who are girls or who are both left-handed and have names beginning with a consonant'. That is,

$$\{k : (k \in \mathrm{G} \cup \mathrm{L}) \text{ and } (k \in \mathrm{G} \cup \mathrm{C})\} \bumpeq \{k : (k \in \mathrm{G}) \text{ or } (k \in \mathrm{L} \cap \mathrm{C})\},$$

i.e.,

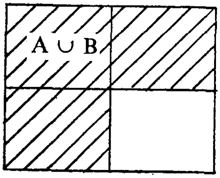
$$(\mathrm{G} \cup \mathrm{L}) \cap (\mathrm{G} \cup \mathrm{C}) \bumpeq \mathrm{G} \cup (\mathrm{L} \cap \mathrm{C}).$$

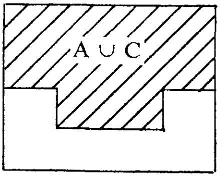
In general we have

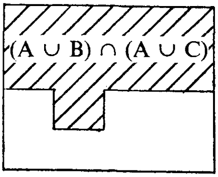
$$(\mathrm{A} \cup \mathrm{B}) \cap (\mathrm{A} \cup \mathrm{C}) \bumpeq \mathrm{A} \cup (\mathrm{B} \cap \mathrm{C})$$

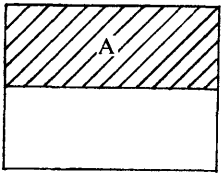
which gives, using the commutative law,

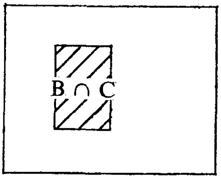
$$(\mathrm{B} \cup \mathrm{A}) \cap (\mathrm{C} \cup \mathrm{A}) \bumpeq (\mathrm{B} \cap \mathrm{C}) \cup \mathrm{A}.$$

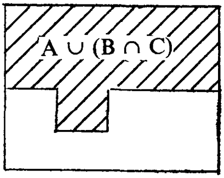












Exercise 22. $\mathrm{A} \cap \mathrm{A} \bumpeq \mathrm{A}$, but $a \times a \neq a$ for any $a \neq 1$.
$\mathrm{A} \cup \mathrm{A} \bumpeq \mathrm{A}$, but $a + a \neq a$ for any $a \neq 0$.

We do have the correspondences:

$$\begin{array}{rclcrcl}
\mathrm{A} \cap \mathrm{B} & \bumpeq & \mathrm{B} \cap \mathrm{A} & \qquad & a \times b & = & b \times a \\
\mathrm{A} \cup \mathrm{B} & \bumpeq & \mathrm{B} \cup \mathrm{A} & & a + b & = & b + a \\
\mathrm{A} \cap (\mathrm{B} \cap \mathrm{C}) & \bumpeq & (\mathrm{A} \cap \mathrm{B}) \cap \mathrm{C} & & a \times (b \times c) & = & (a \times b) \times c \\
\mathrm{A} \cup (\mathrm{B} \cup \mathrm{C}) & \bumpeq & (\mathrm{A} \cup \mathrm{B}) \cup \mathrm{C} & & a + (b + c) & = & (a + b) + c,
\end{array}$$

and even

$$\mathrm{A} \cap (\mathrm{B} \cup \mathrm{C}) \bumpeq (\mathrm{A} \cap \mathrm{B}) \cup (\mathrm{A} \cap \mathrm{C}) \quad a \times (b + c) = a \times b + a \times c,$$

but it is not true that $a + (b \times c) = (a + b) \times (a + c)$, which is the analogue of

$$\mathrm{A} \cup (\mathrm{B} \cap \mathrm{C}) \bumpeq (\mathrm{A} \cup \mathrm{B}) \cap (\mathrm{A} \cup \mathrm{C}).$$

Exercise 23.

$$\begin{aligned}
\mathrm{A} \cap (\mathrm{B} \cup \tilde{\mathrm{A}}) &\bumpeq (\mathrm{A} \cap \mathrm{B}) \cup (\mathrm{A} \cap \tilde{\mathrm{A}}) \\
&\bumpeq (\mathrm{A} \cap \mathrm{B}) \cup \varnothing \\
&\bumpeq \mathrm{A} \cap \mathrm{B}.
\end{aligned}$$

$$\begin{aligned} A\cup(A\cap B) &\bumpeq (A\cup A)\cap(A\cup B)\\ &\bumpeq A\cap(A\cup B).\\ A\subseteq A\cup(A\cap B) &\bumpeq A\cap(A\cup B)\subseteq A, \end{aligned}$$

whence $A\cup(A\cap B)\bumpeq A\cap(A\cup B)\bumpeq A.$

$$\begin{aligned} A\cup(B\cap\tilde{B}) &\bumpeq A\cup\emptyset\bumpeq A.\\ A\cup(B\cap U) &\bumpeq A\cup B.\\ (A\cup B)\cap(A\cup\tilde{B}) &\bumpeq A\cup(B\cap\tilde{B})\bumpeq A\cup\emptyset\bumpeq A. \end{aligned}$$

These may also be simplified by using the definitions in terms of elements, e.g.,

$$\begin{aligned} A\cap(B\cup\tilde{A}) &\bumpeq \{k : k\in A \text{ and } k\in(B\cup\tilde{A})\}\\ &\bumpeq \{k : k\in A \text{ and } (k\in B \text{ or } k\notin A)\}\\ &\bumpeq \{k : (k\in A \text{ and } k\notin A) \text{ or } (k\in A \text{ and } k\in B)\}\\ &\bumpeq \{k : k\in\emptyset \text{ or } k\in A\cap B\}\\ &\bumpeq A\cap B. \end{aligned}$$

Exercise 24. $\tilde{A}\bumpeq\{k : k\in U \text{ but } k\notin A\}\bumpeq U-A.$

Exercise 25. (i) $A-A\bumpeq\{k : k\in A \text{ but } k\notin A\}\bumpeq\emptyset.$

(ii) $A-B\bumpeq\{k : k\in A \text{ but } k\notin B\}$
$\bumpeq\{k : k\in A \text{ and } k\in\tilde{B}\}.$

If $A-B\bumpeq\emptyset$, then no element can belong to both A and $\tilde{B}$, i.e., every element of A must also belong to B, i.e., if $k\in A$ then also $k\in B$, thus $A\subseteq B$.

Exercise 26.

$L-S\bumpeq L\cap\tilde{S}\bumpeq$ {*Anne*, *Bill*, *Jack*, *Lucy*, *Mary*, *Vera*}.

$S-V\bumpeq S\cap\tilde{V}\bumpeq S\cap C\bumpeq$ {*Charles*, *Fred*, *Harry*, *Quentin*}
$\bumpeq S.$

$V-S\bumpeq V\cap\tilde{S}\bumpeq V$, since every element of V is an element of $\tilde{S}$.

$G-V\bumpeq$ {*Dorothy*, *Karen*, *Lucy*, *Mary*, *Nancy*, *Susan*, *Vera*, *Yolande*}.

$(G-V)-S\bumpeq(G-V)\cap\tilde{S}\bumpeq G-V$, since every girl, and *a fortiori* every element of $G-V$, is an element of $\tilde{S}$.

Since
$$\begin{aligned} V-S &\bumpeq V,\\ G-(V-S) &\bumpeq G-V\\ &\bumpeq (G-V)-S \end{aligned}$$

by the previous exercise.

Exercise 27. $A-B \bumpeq A \cap \tilde{B}$, $B-A \bumpeq B \cap \tilde{A}$. These two subsets are in general not equal. To show that '$-$' is not commutative, we need only produce one pair of subsets A, B for which

$$A-B \not\bumpeq B-A.$$

Take A as any proper subset, and $B \bumpeq \varnothing$.
Then $A-B \bumpeq A \cap \tilde{\varnothing} \bumpeq A \cap U \bumpeq A$, while $B-A \bumpeq \varnothing \cap \tilde{A} \bumpeq \varnothing$. Since $\varnothing \subset A$, these two sets are not the same.

Exercise 28. In Exercise 26, it was shown that $G-(V-S) \bumpeq (G-V)-S$, and we may suspect that '$-$' is associative. In general, we have

$$\begin{aligned} A-(B-C) &\bumpeq A-(B \cap \tilde{C}) \\ &\bumpeq A \cap \widetilde{(B \cap \tilde{C})} \\ &\bumpeq A \cap (\tilde{B} \cup C), \end{aligned}$$

using the result for the complement of an intersection.

$$\begin{aligned} (A-B)-C &\bumpeq (A \cap \tilde{B})-C \\ &\bumpeq (A \cap \tilde{B}) \cap \tilde{C} \\ &\bumpeq A \cap (\tilde{B} \cap \tilde{C}), \end{aligned}$$

using the associative law for $\cap$. Now usually $\tilde{B} \cap \tilde{C} \subset \tilde{B} \subset \tilde{B} \cup C$, so we expect that $(A-B)-C \bumpeq A \cap (\tilde{B} \cap \tilde{C}) \subset A \cap (\tilde{B} \cup C) \bumpeq A-(B-C)$, i.e., that the associative law is not in general true. Again we make a choice for A, B, C which produces the desired result. We choose B, C so that

$$\tilde{B} \cap \tilde{C} \subset \tilde{B} \cup C,$$

one choice being $B \bumpeq C$, whence

$$\tilde{B} \bumpeq \tilde{B} \cap \tilde{C} \subset \tilde{B} \cup C \bumpeq U,$$

provided that $B \not\bumpeq \varnothing$ (in which case $\tilde{B} \bumpeq U \not\subset U$).

We now choose A so that

$$A \cap \tilde{B} \not\bumpeq A \cap U,$$

and for this any subset strictly containing $\tilde{B}$ will suffice—since $B \not\bumpeq \varnothing$, $\tilde{B} \subset U$ and such subsets A exist. For this choice of A, B, C,

$$(A-B)-C \bumpeq \tilde{B} \subset A \bumpeq A-(B-C).$$

Hence '$-$' is not an associative operation.

Exercise 29.

$$\begin{aligned} &\text{If } \mathrm{B} \subseteq \mathrm{A},\ \mathrm{A}-\mathrm{B} \bumpeq \{\text{elements of A with all elements of B removed}\},\\ &\text{so}\quad \mathrm{A}-(\mathrm{A}-\mathrm{B}) \bumpeq \{\text{elements of A with all elements not belonging to B removed}\}\\ &\qquad\qquad\qquad \bumpeq \{\text{elements of A which are elements of B}\}\\ &\qquad\qquad\qquad \bumpeq \{\text{elements of B}\}\\ &\qquad\qquad\qquad \bumpeq \mathrm{B}. \end{aligned}$$

Exercise 30. $\mathrm{A}-(\mathrm{A}-\mathrm{B})$ and $(\mathrm{A}-\mathrm{A})-\mathrm{B}$ are not the same set for arbitrary A, B. For example, if $\varnothing \subset \mathrm{B} \subset \mathrm{A}$,

$$\mathrm{A}-(\mathrm{A}-\mathrm{B}) \bumpeq \mathrm{B} \text{ by Ex. 29,}$$

while

$$(\mathrm{A}-\mathrm{A})-\mathrm{B} \bumpeq \varnothing-\mathrm{B} \bumpeq \varnothing.$$

[This example cannot be used if we cannot choose the sets B and A distinct from each other and from $\varnothing$, but this can occur only when U has one element, which is a rather uninteresting case.]

Exercise 31.

$$\begin{aligned} \mathrm{A}-(\mathrm{B} \cup \mathrm{C}) &\bumpeq \{k : k \in \mathrm{A} \text{ but } k \notin (\mathrm{B} \text{ or } \mathrm{C})\}\\ &\bumpeq \{k : k \in \mathrm{A} \text{ and } (k \notin \mathrm{B} \text{ or } k \notin \mathrm{C})\}\\ &\bumpeq \{k : (k \in \mathrm{A} \text{ and } k \notin \mathrm{B}) \text{ or } (k \in \mathrm{A} \text{ and } k \notin \mathrm{C})\}\\ &\bumpeq \{k : (k \in \mathrm{A}-\mathrm{B}) \text{ or } (k \in \mathrm{A}-\mathrm{C})\}\\ &\bumpeq (\mathrm{A}-\mathrm{B}) \cup (\mathrm{A}-\mathrm{C}). \end{aligned}$$

This shows that a distributive law holds between $-$ and $\cup$. Since $-$ is not commutative, we cannot replace $\mathrm{A}-(\mathrm{B} \cup \mathrm{C})$ by $(\mathrm{B} \cup \mathrm{C})-\mathrm{A}$, so we can only use this distributive law in the form in which we have derived it. As the '$-$' symbol appears to the left of the $\cup$ symbol, we say that set-difference is left-distributive over union.

To assert that '$-$' is right-distributive over $\cup$ is to assert the validity of

$$(\mathrm{A} \cup \mathrm{B})-\mathrm{C} \bumpeq (\mathrm{A}-\mathrm{C}) \cup (\mathrm{B}-\mathrm{C}).$$

Is this relation valid?

$$\begin{aligned} \mathrm{A}-(\mathrm{B} \cap \mathrm{C}) &\bumpeq \{k : k \in \mathrm{A} \text{ but } (k \notin \mathrm{B} \cap \mathrm{C})\}\\ &\bumpeq \{k : k \in \mathrm{A} \text{ and } (k \in \tilde{\mathrm{B}} \text{ or } k \in \tilde{\mathrm{C}})\}\\ &\bumpeq \{k : (k \in \mathrm{A} \text{ and } k \in \tilde{\mathrm{B}}) \text{ or } (k \in \mathrm{A} \text{ and } k \in \tilde{\mathrm{C}})\}\\ &\bumpeq \{k : k \in (\mathrm{A}-\mathrm{B}) \text{ or } k \in (\mathrm{A}-\mathrm{C})\}\\ &\bumpeq (\mathrm{A}-\mathrm{B}) \cup (\mathrm{A}-\mathrm{C}). \end{aligned}$$

Since, in general, $(\mathrm{A}-\mathrm{B}) \cap (\mathrm{A}-\mathrm{C}) \subset (\mathrm{A}-\mathrm{B}) \cup (\mathrm{A}-\mathrm{C})$, there is not a left-distributive law for $-$ over $\cap$. If $-$ were right-distributive over $\cap$, we should have

$$(A \cap B) - C \bumpeq (A - C) \cap (B - C).$$

Is this a true relation for all A, B, C?

Exercise 32.

$$\begin{aligned} A \cap (B - C) &\bumpeq \{k : k \in A \text{ and } k \in (B - C)\} \\ &\bumpeq \{k : k \in A \text{ and } (k \in B \text{ and } k \notin C)\} \\ &\bumpeq \{k : (k \in A \text{ and } k \in B) \text{ and } k \notin C\} \\ &\bumpeq \{\text{elements of } A \cap B \text{ except those which} \in C\} \\ &\bumpeq \{\text{elements of } A \cap B \text{ except those which} \in A \cap C\}, \end{aligned}$$

since any element of C which does not belong to A cannot belong to $A \cap B$;

$$\bumpeq (A \cap B) - (A \cap C).$$

Thus, since $\cap$ is commutative, and

$$A \cap (B - C) \bumpeq (B - C) \cap A,$$

we say that $\cap$ is distributive over $-$.

$A \subseteq A \cup (B - C)$, while A may not be a subset of $(A \cup B) - (A \cup C)$. For example, take $B \bumpeq C$, and $A \not\bumpeq \emptyset$. Then

$$A \cup (B - C) \bumpeq A \cup (B - B) \bumpeq A \cup \emptyset \bumpeq A,$$

while $(A \cup B) - (A \cup C) \bumpeq (A \cup B) - (A \cup B) \bumpeq \emptyset$.

Hence $\cup$ is not distributive over $-$.

Exercise 33.

$$A\,\sigma\,(B\,\sigma\,C) \bumpeq \tilde{A} \cup (\tilde{B} \cup C).$$

$$\begin{aligned} (A\,\sigma\,B)\,\sigma\,C &\bumpeq \widetilde{(\tilde{A} \cup B)} \cup C \\ &\bumpeq (A \cap \tilde{B}) \cup C \\ &\subseteq \tilde{B} \cup C \\ &\subseteq \tilde{A} \cup (\tilde{B} \cup C) \\ &\bumpeq A\,\sigma\,(B\,\sigma\,C). \end{aligned}$$

Thus $A\,\sigma\,(B\,\sigma\,C) \supseteq (A\,\sigma\,B)\,\sigma\,C$.

(a) If $A \subseteq \tilde{C}$, $B \subseteq \tilde{C}$ then $\tilde{B} \supseteq C$, $\tilde{A} \supseteq C$,

and $A\,\sigma\,(B\,\sigma\,C) \supset C$ unless $\tilde{A} \bumpeq \tilde{B} \bumpeq C$, when $A\,\sigma\,(B\,\sigma\,C) \bumpeq C$. If $A \subset B$, $A \cap \tilde{B} \subseteq B \cap \tilde{B} \bumpeq \emptyset$, and so $(A\,\sigma\,B)\,\sigma\,C \bumpeq \emptyset \cup C \bumpeq C$.

Thus by choosing $A \subset B \subset \tilde{C}$, we have

$$(A\,\sigma\,B)\,\sigma\,C \subset A\,\sigma\,(B\,\sigma\,C).$$

(b) Choose the subsets so that $A \subseteq B \subset C \subset U$, then

$$(A\,\sigma\,B)\,\sigma\,C \bumpeq C \subset U \bumpeq A\,\sigma\,(B\,\sigma\,C).$$

(c) Choose A so that $A \subset C$.

Exercise 34.

$$\begin{aligned} (A-B)\,\sigma\,A &\bumpeq \widetilde{(A \cap \tilde{B})} \cup A \\ &\bumpeq (\tilde{A} \cup B) \cup A \\ &\bumpeq (B \cup \tilde{A}) \cup A \\ &\bumpeq B \cup (\tilde{A} \cup A) \\ &\bumpeq B \cup U \\ &\bumpeq U. \end{aligned}$$

Exercise 35.

$$A\,\sigma\,(B-A) \bumpeq \tilde{A} \cup (B \cap \tilde{A}).$$

But $B \cap \tilde{A} \subseteq \tilde{A}$, hence $A\,\sigma\,(B-A) \bumpeq \tilde{A}$.

Exercise 36.

$$\begin{aligned} (A \cup B)\,\sigma\,C &\bumpeq \widetilde{(A \cup B)} \cup C \\ &\bumpeq (\tilde{A} \cap \tilde{B}) \cup C \\ &\bumpeq (\tilde{A} \cup C) \cap (\tilde{B} \cup C) \quad \text{(distributive law)} \\ &\bumpeq (A\,\sigma\,C) \cap (B\,\sigma\,C). \end{aligned}$$

$$\begin{aligned} A\,\sigma\,(B \cup C) &\bumpeq \tilde{A} \cup (B \cup C) \\ &\bumpeq (\tilde{A} \cup B) \cup C \\ &\bumpeq (A\,\sigma\,B) \cup C. \end{aligned}$$

$$\begin{aligned} (A \cap B)\,\sigma\,C &\bumpeq \widetilde{(A \cap B)} \cup C \\ &\bumpeq (\tilde{A} \cup \tilde{B}) \cup C \\ &\bumpeq \tilde{A} \cup (B\,\sigma\,C). \end{aligned}$$

$$\begin{aligned} A\,\sigma\,(B \cap C) &\bumpeq \tilde{A} \cup (B \cap C) \\ &\bumpeq (\tilde{A} \cup B) \cap (\tilde{A} \cup C) \\ &\bumpeq (A\,\sigma\,B) \cap (A\,\sigma\,C). \end{aligned}$$

That is, σ is left-distributive over $\cap$.

$$A\,\sigma\,\tilde{A} \bumpeq \tilde{A} \cup \tilde{A} \bumpeq \tilde{A}.$$

Exercise 37.

$$\begin{aligned} (A\,\sigma\,B) \cap (B\,\sigma\,C) &\bumpeq (\tilde{A} \cup B) \cap (\tilde{B} \cup C) \\ &\bumpeq (\tilde{A} \cap (\tilde{B} \cup C)) \cup (B \cap (\tilde{B} \cup C)) \text{ using the} \end{aligned}$$

distributive law,

$$\bumpeq (\tilde{A} \cap (\tilde{B} \cup C)) \cup ((B \cap \tilde{B}) \cup (B \cap C)).$$

Now $\tilde{A} \cap (\tilde{B} \cup C) \subseteq \tilde{A}$, $B \cap \tilde{B} \bumpeq \varnothing$, $B \cap C \subseteq C$,

so $\quad (A\,\sigma\,B) \cap (B\,\sigma\,C) \subseteq \tilde{A} \cup (\varnothing \cup C) \bumpeq \tilde{A} \cup C \bumpeq A\,\sigma\,C.$

This exercise will have application in Ch. 3.

Exercise 38. Each subset or its complement appears as a factor in a primary subset. For n subsets, we have 2^n possible combinations and so 2^n primary subsets.

Exercise 39. We know that $S \subset C$, $S \subset \tilde{G}$ and therefore we can simplify some of the expressions for the $16(= 2^4)$ primary subsets.

Since $S \subset C$, then $S \cap \tilde{C} \bumpeq S \cap V \bumpeq \varnothing$, so all primary subsets involving $S \cap \tilde{C}$ reduce to the null set. There are four of these.

Since $S \subset \tilde{G}$, $S \cap \tilde{\tilde{G}} \bumpeq S \cap G \bumpeq \varnothing$, so all primary subsets involving $S \cap G$ are the null set. There are four of these.
There are ten remaining primary subsets to be found:

$$\begin{aligned}
\tilde{G} \cap L \cap S \cap C &\bumpeq \tilde{G} \cap L \cap S \\
&\bumpeq L \cap S && (S \subset \tilde{G}) \\
\tilde{G} \cap \tilde{L} \cap S \cap C &\bumpeq \tilde{L} \cap S \\
G \cap L \cap \tilde{S} \cap C &\bumpeq G \cap L \cap C && (\tilde{S} \supset G) \\
\tilde{G} \cap L \cap \tilde{S} \cap C &\bumpeq \tilde{G} \cap L \cap \tilde{S} \\
G \cap \tilde{L} \cap \tilde{S} \cap C &\bumpeq G \cap \tilde{L} \cap C \\
\tilde{G} \cap \tilde{L} \cap \tilde{S} \cap C &\bumpeq \tilde{G} \cap \tilde{L} \cap \tilde{S} \\
G \cap L \cap \tilde{S} \cap \tilde{C} &\bumpeq L \cap \tilde{C}.
\end{aligned}$$

Since also $\quad \tilde{G} \cap \tilde{C} \bumpeq B \cap V \bumpeq \varnothing$,

$$\tilde{G} \cap L \cap \tilde{S} \cap \tilde{C} \bumpeq \varnothing$$

and $\tilde{G} \cap \tilde{L} \cap \tilde{S} \cap \tilde{C} \bumpeq \varnothing$.

Finally,

$$G \cap \tilde{L} \cap \tilde{S} \cap \tilde{C} \bumpeq \tilde{L} \cap \tilde{C}.$$

Exercise 40. There are 2^n primary subsets, and each may be chosen or rejected in forming a union of such subsets. The total number of such unions is thus $2^{(2^n)} = 2^{2^n}$. Since the primary subsets are not necessarily distinct, these subsets are not necessarily all distinct.

Chapter 4

Exercise 1. (i) Axiom 8 gives, after using axiom 5,

$$\tilde{A} \cup A \leftrightharpoons U \text{ and } \tilde{A} \cap A \leftrightharpoons \varnothing.$$

Thus, since a complement is unique, A is the complement of $\tilde{A}$. But the complement of $\tilde{A}$ is written $\tilde{\tilde{A}}$. Hence $\tilde{\tilde{A}} \leftrightharpoons A$.

(ii) By axiom 8,

$$\begin{aligned} U &\leftrightharpoons A \cup \tilde{A} \\ &\leftrightharpoons A \cup (\tilde{A} \cap U) && \text{by axiom 7} \\ &\leftrightharpoons (A \cup \tilde{A}) \cap (A \cup U) && \text{by axiom 6} \\ &\leftrightharpoons U \cap (A \cup U) && \text{by axiom 8} \\ &\leftrightharpoons A \cup U && \text{by axiom 7} \end{aligned}$$

Hence by duality $A \cap \varnothing = \varnothing$.

(iii) (a) By Ex. (ii),

$$\begin{aligned} A \cup A &\leftrightharpoons (A \cup A) \cup U \\ &\leftrightharpoons A \cup (A \cup U) && \text{(axiom 4),} \\ &\leftrightharpoons A \cup U && \text{(Ex. (ii)),} \\ &\leftrightharpoons A && \text{(Ex. (ii)).} \end{aligned}$$

Hence by duality $A \cap A \leftrightharpoons A$.

In §4.6, we need a proof of $A \cup A \leftrightharpoons A$ which does not use axiom 4. We have the following alternative proof.

$$\begin{aligned} A \leftrightharpoons A \cup \varnothing \leftrightharpoons A \cup (A \cap \tilde{A}) &\leftrightharpoons (A \cup A) \cap (A \cup \tilde{A}) \\ &\leftrightharpoons (A \cup A) \cap U \leftrightharpoons A \cup A. \end{aligned}$$

(b) If $A \cup B \leftrightharpoons \varnothing$, then

$$A \leftrightharpoons A \cup \varnothing \leftrightharpoons A \cup (A \cup B) \leftrightharpoons (A \cup A) \cup B \leftrightharpoons A \cup B \leftrightharpoons \varnothing,$$

and similarly $B \leftrightharpoons \varnothing$.

If $A \cap B \leftrightharpoons U$, then

$$A \leftrightharpoons A \cap U \leftrightharpoons A \cap (A \cap B) \leftrightharpoons (A \cap A) \cap B \leftrightharpoons A \cap B \leftrightharpoons U,$$

and similarly $B \leftrightharpoons U$.

(iv)
$$\begin{aligned} (A \cup (A \cap B)) \cap \tilde{A} &\leftrightharpoons \tilde{A} \cap (A \cup (A \cap B)) \\ &\leftrightharpoons (\tilde{A} \cap A) \cup (\tilde{A} \cap (A \cap B)) \\ &\leftrightharpoons \varnothing \cup (\tilde{A} \cap A) \cap B \\ &\leftrightharpoons \varnothing \cup (\varnothing \cap B) \\ &\leftrightharpoons \varnothing \cup \varnothing && \text{(Ex. (ii))} \\ &\leftrightharpoons \varnothing. \\ (A \cup (A \cap B)) \cup \tilde{A} &\leftrightharpoons (A \cup \tilde{A}) \cup (A \cap B) \\ &\leftrightharpoons U \cup (A \cap B) \\ &\leftrightharpoons U && \text{(Ex. (ii)).} \end{aligned}$$

So $\tilde{A}$ is the complement of $A \cup (A \cap B)$, hence, since the complement is unique,

$$A \cup (A \cap B) \leftrightharpoons A.$$

By duality $A \cap (A \cup B) \leftrightharpoons A$, or otherwise we have

$$A \cup (A \cap B) \leftrightharpoons (A \cup A) \cap (A \cup B) \leftrightharpoons A \cap (A \cup B) \text{ (Ex. (iii))}.$$

(v) We show that $\tilde{A} \cap \tilde{B}$ is the complement of $A \cup B$ by proving

$$(A \cup B) \cup (\tilde{A} \cap \tilde{B}) \leftrightharpoons U \text{ and } (A \cup B) \cap (\tilde{A} \cap \tilde{B}) \leftrightharpoons \varnothing.$$

Firstly,

$$\begin{aligned}
(A \cup B) \cup (\tilde{A} \cap \tilde{B}) &\leftrightharpoons A \cup (B \cup (\tilde{A} \cap \tilde{B})) && \text{(assoc. law)}\\
&\leftrightharpoons A \cup ((B \cup \tilde{A}) \cap (B \cup \tilde{B})) && \text{(distrib. law)}\\
&\leftrightharpoons A \cup ((B \cup \tilde{A}) \cap U) && \text{(axiom 8)}\\
&\leftrightharpoons A \cup (B \cup \tilde{A}) && \text{(axiom 7)}\\
&\leftrightharpoons (A \cup \tilde{A}) \cup B && \text{(axioms 4, 5)}\\
&\leftrightharpoons U \cup B && \text{(axiom 8)}\\
&\leftrightharpoons U. && \text{(Ex. (ii))}
\end{aligned}$$

Secondly,

$$\begin{aligned}
(A \cup B) \cap (\tilde{A} \cap \tilde{B}) &\leftrightharpoons ((A \cup B) \cap \tilde{A}) \cap \tilde{B}\\
&\leftrightharpoons ((A \cap \tilde{A}) \cup (B \cap \tilde{A})) \cap \tilde{B}\\
&\leftrightharpoons (\varnothing \cup (B \cap \tilde{A})) \cap \tilde{B}\\
&\leftrightharpoons (B \cap \tilde{A}) \cap \tilde{B}\\
&\leftrightharpoons \tilde{A} \cap (B \cap \tilde{B})\\
&\leftrightharpoons \tilde{A} \cap \varnothing\\
&\leftrightharpoons \varnothing.
\end{aligned}$$

By duality, $\quad (\widetilde{A \cap B}) \leftrightharpoons \tilde{A} \cup \tilde{B}$.

(vi)

$$\begin{aligned}
&(\tilde{A} \cup B) \cap (A \cup \tilde{B})\\
&\leftrightharpoons \{(\tilde{A} \cup B) \cap A\} \cup \{(\tilde{A} \cup B) \cap \tilde{B})\} && \text{(distributive law)}\\
&\leftrightharpoons \{(\tilde{A} \cap A) \cup (B \cap A)\} \cup \{(\tilde{A} \cap \tilde{B}) \cup (B \cap \tilde{B})\} && \text{(distributive law)}\\
&\leftrightharpoons \{\varnothing \cup (B \cap A)\} \cup \{(\tilde{A} \cap \tilde{B}) \cup \varnothing\}\\
&\leftrightharpoons (B \cap A) \cup (\tilde{A} \cap \tilde{B})
\end{aligned}$$

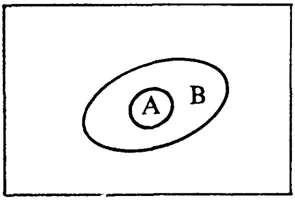
which is the required result, since $B \cap A \leftrightharpoons A \cap B$.

We remark here that the associative laws (axiom 4) enable us if we wish to dispense with parentheses in an expression such as $A \cap (B \cap C)$, since no confusion arises from interpreting $A \cap B \cap C$ either as $A \cap (B \cap C)$ or as $(A \cap B) \cap C$. Similarly, the associative laws enable us to rearrange parentheses in expressions such as $(A \cap B) \cap (C \cap D)$; e.g.,

$$\begin{aligned}
(A \cap B) \cap (C \cap D) &\leftrightharpoons A \cap (B \cap (C \cap D))\\
&\leftrightharpoons ((A \cap B) \cap C) \cap D\\
&\leftrightharpoons (A \cap (B \cap C)) \cap D\\
&\leftrightharpoons A \cap ((B \cap C) \cap D)
\end{aligned}$$

etc., and again no confusion will arise if we write simply $A \cap B \cap C \cap D$ for any of the above expressions. Sometimes in the solutions the use of commutative and associative laws will be explicitly indicated, while otherwise application of them may be incorporated with other operations without statement.

Exercise 2. Using a diagram for $A \subseteq B$ (A, B as subsets):



we see that

$$\begin{aligned} A \cup B &\leftrightharpoons B \\ A \cap B &\leftrightharpoons A \\ A \cap \tilde{B} &\leftrightharpoons \emptyset \\ \tilde{A} \cup B &\leftrightharpoons U. \end{aligned}$$

In our Boolean algebra, we should be able to derive all four conditions from any one. So, if

$$A \cup B \leftrightharpoons B,$$

we have (i) $A \cap B \leftrightharpoons A \cap (A \cup B) \leftrightharpoons A$ by Ex. (iv) above,

(ii) $\tilde{B} \leftrightharpoons \tilde{A} \cap \tilde{B}$ by Ex. (v) above,

hence

$$\begin{aligned} A \cap \tilde{B} &\leftrightharpoons A \cap (\tilde{A} \cap \tilde{B}) \\ &\leftrightharpoons (A \cap \tilde{A}) \cap \tilde{B} \\ &\leftrightharpoons \emptyset \cap \tilde{B} \\ &\leftrightharpoons \emptyset, \end{aligned}$$

and (iii) By (i), $A \leftrightharpoons A \cap B$,

so $\tilde{A} \leftrightharpoons \tilde{A} \cup \tilde{B}$,

hence

$$\begin{aligned} \tilde{A} \cup B &\leftrightharpoons (\tilde{A} \cup \tilde{B}) \cup B \\ &\leftrightharpoons \tilde{A} \cup (\tilde{B} \cup B) \\ &\leftrightharpoons \tilde{A} \cup U \\ &\leftrightharpoons U. \end{aligned}$$

Similarly, we can derive $A \cup B \leftrightharpoons B$ from each of (i), (ii) and (iii).

Exercise 3. (i) $[A \subseteq B] \Leftrightarrow [A \cup B \leftrightharpoons B]$,

$[B \subseteq A] \Leftrightarrow [B \cup A \leftrightharpoons A]$.

So $[A \subseteq B \text{ and } B \subseteq A] \Leftrightarrow [A \cup B \leftrightharpoons B \text{ and } B \cup A \leftrightharpoons A]$.

But $A \cup B \leftrightharpoons B \cup A$, hence

$$B \leftrightharpoons A \cup B \leftrightharpoons B \cup A \leftrightharpoons A,$$

i.e., $\quad A \leftrightharpoons B.$

(ii)

$$\begin{aligned}(A \cap B) \cap A &\leftrightharpoons A \cap (A \cap B)\\ &\leftrightharpoons (A \cap A) \cap B\\ &\leftrightharpoons A \cap B,\end{aligned}$$

so $A \cap B \subseteq A$. Similarly $A \cap B \subseteq B$. $A \cup (A \cup B) \leftrightharpoons (A \cup A) \cup B \leftrightharpoons A \cup B$,

so $A \subseteq A \cup B$. Similarly $B \subseteq A \cup B$. $A \cap B \subseteq A \subseteq A \cup B$, which by Ex. 4 (i) below gives $A \cap B \subseteq A \cup B$. Alternately, we have $(A \cap B) \cap (A \cup B) \leftrightharpoons ((A \cap B) \cap A) \cup ((A \cap B) \cap B) \leftrightharpoons (A \cap B) \cup (A \cap B)$, as above, $\leftrightharpoons A \cap B$

whence the result.

Exercise 4. (i) $[A \subseteq B] \Leftrightarrow [A \cup B \leftrightharpoons B]$,
$[B \subseteq C] \Leftrightarrow [B \cup C \leftrightharpoons C]$,

hence

$$\begin{aligned}[A \subseteq B \text{ and } B \subseteq C] &\Leftrightarrow [A \cup B \leftrightharpoons B \text{ and } B \cup C \leftrightharpoons C]\\ &\Rightarrow [(A \cup B) \cup C \leftrightharpoons C \text{ and } B \cup C \leftrightharpoons C]\\ &\Leftrightarrow [A \cup (B \cup C) \leftrightharpoons C \text{ and } B \cup C \leftrightharpoons C]\\ &\Rightarrow [A \cup C \leftrightharpoons C]\\ &\Leftrightarrow [A \subseteq C].\end{aligned}$$

Hence $[A \subseteq B \text{ and } B \subseteq C] \Rightarrow [A \subseteq C]$.

(ii) If $A \subseteq B$, then $A \cup B \leftrightharpoons B$, and

$$\begin{aligned}(A \cup C) \cup (B \cup C) &\leftrightharpoons (C \cup A) \cup (B \cup C)\\ &\leftrightharpoons C \cup (A \cup (B \cup C))\\ &\leftrightharpoons C \cup ((A \cup B) \cup C)\\ &\leftrightharpoons C \cup (B \cup C)\\ &\leftrightharpoons C \cup (C \cup B)\\ &\leftrightharpoons (C \cup C) \cup B.\\ (C \cup C) \cup B &\leftrightharpoons C \cup B\\ &\leftrightharpoons B \cup C\end{aligned}$$

whence $\quad A \cup C \subseteq B \cup C.$

Similarly, if $A \subseteq B$, $A \cap B \leftrightharpoons A$, and

$$\begin{aligned}(A \cap C) \cap (B \cap C) &\leftrightharpoons (A \cap B) \cap (C \cap C)\\ &\leftrightharpoons A \cap C\end{aligned}$$

whence $\quad A \cap C \subseteq B \cap C.$

Exercise 5. (i) $$U - A \leftrightharpoons U \cap \tilde{A} \leftrightharpoons \tilde{A}.$$

(ii)
$$\begin{aligned} A-(A-B) &\leftrightharpoons A \cap \widetilde{(A-B)} \\ &\leftrightharpoons A \cap \widetilde{(A \cap \tilde{B})} \\ &\leftrightharpoons A \cap (\tilde{A} \cup B) \\ &\leftrightharpoons (A \cap \tilde{A}) \cup (A \cap B) \\ &\leftrightharpoons \varnothing \cup (A \cap B) \\ &\leftrightharpoons A \cap B. \end{aligned}$$

Hence, if $B \subseteq A$, $A \cap B \leftrightharpoons B$ and $A-(A-B) \leftrightharpoons B$.

(iii)
$$\begin{aligned} (A-B)-C &\leftrightharpoons (A \cap \tilde{B}) \cap \tilde{C} \\ &\subseteq A \cap \tilde{B} \\ &\subseteq (A \cap \tilde{B}) \cup (A \cap C) \\ &\leftrightharpoons A \cap (\tilde{B} \cup C) \\ &\leftrightharpoons A \cap \widetilde{(B \cap \tilde{C})} \\ &\leftrightharpoons A \cap (B-C) \\ &\leftrightharpoons A-(B-C). \end{aligned}$$

(iv) $$A - A \leftrightharpoons A \cap \tilde{A} \leftrightharpoons \varnothing.$$

Exercise 6. (i) $A-B \leftrightharpoons A \cap \tilde{B}$, $B-A \leftrightharpoons B \cap \tilde{A}$, and neither is replaceable by the other in general. If we do have, for a given A,
$$A-B \leftrightharpoons B-A$$
then
$$A \cap \tilde{B} \leftrightharpoons B \cap \tilde{A},$$
and so
$$\begin{aligned} A \cap (A \cap \tilde{B}) \leftrightharpoons A \cap (B \cap \tilde{A}) &\leftrightharpoons B \cap (A \cap \tilde{A}) \\ &\leftrightharpoons B \cap \varnothing \leftrightharpoons \varnothing, \end{aligned}$$
but
$$A \cap (A \cap \tilde{B}) \leftrightharpoons (A \cap A) \cap \tilde{B} \leftrightharpoons A \cap \tilde{B},$$
so
$$A \cap \tilde{B} \leftrightharpoons \varnothing.$$
Similarly, $B \cap \tilde{A} \leftrightharpoons \varnothing$, which by complementation gives $A \cup \tilde{B} \leftrightharpoons U$.

Hence, since
$$A \cap \tilde{B} \leftrightharpoons \varnothing,\ A \cup \tilde{B} \leftrightharpoons U,$$
we have
$$\tilde{A} \leftrightharpoons \tilde{B}, \text{ and so } A \leftrightharpoons B.$$

(ii) By examining the proof of Ex. 5 (iii), we see that '$-$' is not in general associative. If $A \cap C \leftrightharpoons \varnothing$,

then
$$A \cap \tilde{B} \leftrightharpoons (A \cap \tilde{B}) \cup (A \cap C),$$
and so
$$(A-B)-C \leftrightharpoons A-(B-C)$$

if and only if $\qquad A \cap \tilde{B} \cap \tilde{C} \leftrightharpoons A \cap \tilde{B}$,

i.e., if and only if $A \cap \tilde{B} \subseteq \tilde{C}$. But if $A \cap C \leftrightharpoons \emptyset$, then $A \subseteq \tilde{C}$, and so $A \cap \tilde{B} \subseteq \tilde{C}$. Hence if $A \cap C \leftrightharpoons \emptyset$,

$$(A-B)-C \leftrightharpoons A-(B-C)$$

for all B.

Exercise 7.

(i) (a) $A \cap (B-C) \leftrightharpoons A \cap (B \cap \tilde{C}) \leftrightharpoons A \cap B \cap \tilde{C}$.

$$\begin{aligned}(A \cap B) - (A \cap C) &\leftrightharpoons (A \cap B) \cap (\widetilde{A \cap C})\\ &\leftrightharpoons (A \cap B) \cap (\tilde{A} \cup \tilde{C})\\ &\leftrightharpoons ((A \cap B) \cap \tilde{A}) \cup ((A \cap B) \cap \tilde{C})\\ &\leftrightharpoons ((A \cap \tilde{A}) \cap B) \cup (A \cap B \cap \tilde{C})\\ &\leftrightharpoons (\emptyset \cap B) \cup (A \cap B \cap \tilde{C})\\ &\leftrightharpoons \emptyset \cup (A \cap B \cap \tilde{C})\\ &\leftrightharpoons A \cap B \cap \tilde{C},\end{aligned}$$

so $\qquad A \cap (B-C) \leftrightharpoons (A \cap B) - (A \cap C)$.

(b) $\qquad (A \cap B)-C \leftrightharpoons A \cap B \cap \tilde{C}$.

$$\begin{aligned}(A-C) \cap (B-C) &\leftrightharpoons (A \cap \tilde{C}) \cap (B \cap \tilde{C})\\ &\leftrightharpoons (A \cap \tilde{C}) \cap B \cap \tilde{C}\\ &\leftrightharpoons A \cap B \cap \tilde{C} \cap \tilde{C}\\ &\leftrightharpoons A \cap B \cap \tilde{C}\end{aligned}$$

whence the result, and (c) follows.

(a) states that $\cap$ is distributive over $-$,

(b) states that $-$ is right-distributive over $\cap$.

Since $-$ is not commutative, we must preserve the order of factors in terms. Here, the $-$ operation is on the right of the $\cap$ operation. To assert that $-$ is left-distributive over $\cap$ is to assert that

$$C-(A \cap B) \rightleftharpoons (C-A) \cap (C-B),$$

and we shall see below that this is false.

(ii)
$$\begin{aligned}(A \cup B)-C &\rightleftharpoons (A \cup B) \cap \tilde{C}\\ &\rightleftharpoons (A \cap \tilde{C}) \cup (B \cap \tilde{C})\\ &\rightleftharpoons (A-C) \cup (B-C)\end{aligned}$$

i.e., $-$ is right-distributive over $\cup$.

$$A \cup (B-C) \leftrightharpoons A \cup (B \cap \tilde{C}).$$

$$\begin{aligned}(A \cup B) - (A \cup C) &\leftrightharpoons (A \cup B) \cap \widetilde{(A \cup C)},\\ &\leftrightharpoons (A \cup B) \cap (\tilde{A} \cap \tilde{C})\\ &\leftrightharpoons (A \cap \tilde{A} \cap \tilde{C}) \cup (\tilde{A} \cap \tilde{C} \cap B),\\ &\leftrightharpoons \tilde{A} \cap (B \cap \tilde{C}),\\ &\subseteq A \cup (B \cap \tilde{C})\end{aligned}$$

and in general $\leftrightharpoons$ cannot replace $\subseteq$ in the last step. Hence the given result is not always valid. When is it valid?

$$\begin{aligned}\text{(iii) } A - (B \cup C) \leftrightharpoons A \cap \widetilde{(B \cup C)} &\leftrightharpoons A \cap (\tilde{B} \cap \tilde{C})\\ &\leftrightharpoons (A \cap \tilde{B}) \cap \tilde{C}\\ &\leftrightharpoons (A - B) \cap \tilde{C}\\ &\leftrightharpoons (A - B) - C.\end{aligned}$$

$$\begin{aligned}A - (B \cap C) &\leftrightharpoons A \cap \widetilde{(B \cap C)}\\ &\leftrightharpoons A \cap (\tilde{B} \cup \tilde{C})\\ &\leftrightharpoons (A \cap \tilde{B}) \cup (A \cap \tilde{C})\\ &\leftrightharpoons (A - B) \cup (A - C).\end{aligned}$$

If $-$ were left-distributive over $\cap$, we should have

$$A - (B \cap C) \leftrightharpoons (A - B) \cap (A - C),$$

which gives, with the above result,

$$(A - B) \cap (A - C) \leftrightharpoons (A - B) \cup (A - C)$$

a result which is in general false. Thus, the left-distributive law for $-$ over $\cap$ is false.

Exercise 8. (i)
$$\begin{aligned}A + \emptyset &\leftrightharpoons (A - \emptyset) \cup (\emptyset - A)\\ &\leftrightharpoons (A \cap U) \cup (\emptyset \cap \tilde{A})\\ &\leftrightharpoons A \cup \emptyset\\ &\leftrightharpoons A.\end{aligned}$$

(ii)
$$\begin{aligned}A + U &\leftrightharpoons (A - U) \cup (U - A)\\ &\leftrightharpoons (A \cap \emptyset) \cup (U \cap \tilde{A})\\ &\leftrightharpoons \emptyset \cup \tilde{A}\\ &\leftrightharpoons \tilde{A}.\end{aligned}$$

(iii)
$$\begin{aligned}A + A &\leftrightharpoons (A - A) \cup (A - A)\\ &\leftrightharpoons \emptyset \cup \emptyset\\ &\leftrightharpoons \emptyset.\end{aligned}$$

(iv) (a) If $A \leftrightharpoons B$, (iii) gives $A + B \leftrightharpoons \emptyset$.

(b) If $A+B \leftrightharpoons \varnothing$, then $(A-B)\cup(B-A) \leftrightharpoons \varnothing$, hence
$A-B \leftrightharpoons \varnothing$ and $B-A \leftrightharpoons \varnothing$, so
$A-B \leftrightharpoons B-A$, so by Ex. 6 (i), $A \leftrightharpoons B$.

Exercise 9. (i)
$$\begin{aligned} A+B &\leftrightharpoons (A-B)\cup(B-A)\\ &\leftrightharpoons (B-A)\cup(A-B) \text{ since } \cup \text{ is commutative,}\\ &\leftrightharpoons B+A. \end{aligned}$$

(ii) We shall make use of Ex. 1 (vi) in the complementary form of its dual, viz.:

$$\widetilde{(A\cap\tilde{B})\cup(B\cap\tilde{A})} \leftrightharpoons (A\cap B)\cup(\tilde{A}\cap\tilde{B}). \qquad (*)$$

We have
$$\begin{aligned} A+(B+C) &\leftrightharpoons [A-(B+C)]\cup[(B+C)-A]\\ &\leftrightharpoons [A\cap\widetilde{\{(B\cap\tilde{C})\cup(\tilde{B}\cap C)\}}]\cup\\ &\qquad\qquad [\{(B\cap\tilde{C})\cup(\tilde{B}\cap C)\}\cap\tilde{A}]\\ &\leftrightharpoons [A\cap\{(B\cap C)\cup(\tilde{B}\cap\tilde{C})\}]\cup\\ &\qquad\qquad [\{(B\cap\tilde{C})\cup(\tilde{B}\cap C)\}\cap\tilde{A}], \end{aligned}$$
using (*);
$$\begin{aligned} &\leftrightharpoons [\{A\cap(B\cap C)\}\cup\{A\cap(\tilde{B}\cap\tilde{C})\}]\cup\\ &\qquad [\{(B\cap\tilde{C})\cap\tilde{A}\}\cup\{(\tilde{B}\cap C)\cap\tilde{A}\}] \end{aligned}$$
(using the distributive laws);
$$\begin{aligned} &\leftrightharpoons [\{(A\cap\tilde{B})\cap\tilde{C}\}\cup\{(B\cap\tilde{A})\cap\tilde{C}\}]\cup[\{C\cap(A\cap B)\}\cup\\ &\qquad\qquad \{C\cap(\tilde{A}\cap\tilde{B})\}] \end{aligned}$$
using the commutative law for $\cup$ and associative law for $\cap$,
$$\leftrightharpoons [\{(A\cap\tilde{B})\cup(B\cap\tilde{A})\}\cap\tilde{C}]\cup[C\cap\{(A\cap B)\cup(\tilde{A}\cap\tilde{B})\}]$$
using the distributive law for $\cap$,
$$\leftrightharpoons [(A+B)\cap\tilde{C}]\cup[C\cap\widetilde{(A+B)}]$$
using (*) again,
$$\leftrightharpoons (A+B)+C.$$

(iii) $B+C \leftrightharpoons B+(A+B) \leftrightharpoons B+B+A \leftrightharpoons \varnothing+A \leftrightharpoons A.$

Exercise 10.

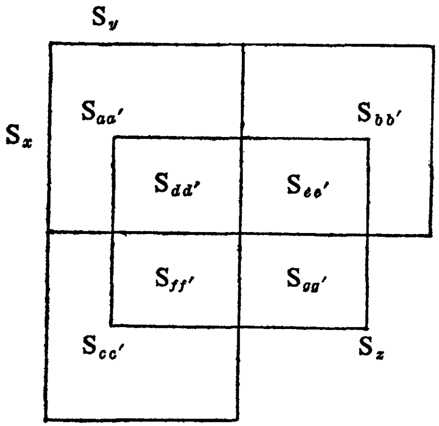
(i)
$$\begin{aligned} (A\cap B)+(A\cap C) &\rightleftharpoons \{(A\cap B)\cap\widetilde{(A\cap C)}\}\cup\\ &\qquad\qquad \{(A\cap C)\cap\widetilde{(A\cap B)}\}\\ &\rightleftharpoons \{(A\cap B)\cap(\tilde{A}\cup\tilde{C})\}\cup\\ &\qquad\qquad \{(A\cap C)\cap(\tilde{A}\cup\tilde{B})\}\\ &\rightleftharpoons (A\cap B\cap\tilde{A})\cup(A\cap B\cap\tilde{C})\cup\\ &\qquad\qquad (A\cap C\cap\tilde{A})\cup(A\cap C\cap\tilde{B} \end{aligned}$$

$$
\begin{aligned}
&\rightleftharpoons \emptyset \cup (A \cap (B \cap \tilde{C})) \cup \emptyset \cup (A \cap (C \cap \tilde{B}))\\
&\rightleftharpoons A \cap \{(B \cap \tilde{C}) \cup (\tilde{B} \cap C)\},\\
&\rightleftharpoons A \cap (B+C).
\end{aligned}
$$

$$
\begin{aligned}
\text{(ii) } (A \cup B)+(A \cup C) &\rightleftharpoons \{(A \cup B) \cap (\widetilde{A \cup C})\} \cup \{(A \cup C) \cap (\widetilde{A \cup B})\}\\
&\rightleftharpoons \{(A \cup B) \cap (\tilde{A} \cap \tilde{C})\} \cup \{(A \cup C) \cap (\tilde{A} \cap \tilde{B})\}\\
&\rightleftharpoons (B \cap \tilde{A} \cap \tilde{C}) \cup (C \cap \tilde{A} \cap \tilde{B})\\
&\rightleftharpoons \tilde{A} \cap ((B \cap \tilde{C}) \cup (C \cap \tilde{B}))\\
&\rightleftharpoons A \cap (B+C)\\
&\subseteq B+C\\
&\subseteq A \cup (B+C).
\end{aligned}
$$

Chapter 5

Exercise 3. The Venn diagram is:



$$
\begin{aligned}
x &= abdea'b'd'e'\\
y &= acdfa'c'd'f'\\
z &= defgd'e'f'g'\\
d' &= a'b'c'e'f'g'\\
j(x, y) &= bcef\,b'c'e'f'\\
l[j(x, y), z] &= bcdefgd'e'f'g'\\
h[j(x, y), z] &= efb'c'e'f'\\
j[j(x, y), z] &= g'd'/b'c'.
\end{aligned}
$$

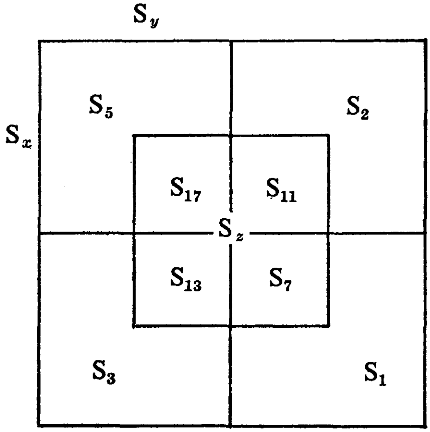
Similarly

$$j[j(x, z), y] = c'd'/b'g' \neq j[j(x, y), z].$$

Exercise 4. (i) Since N $=$ 1.2.3.5.7.11.13.17

$$S_N \bumpeq \{2, 3, 5, 7, 11, 13, 17\}$$

the subsets S_i being non-intersecting. We may take these eight subsets therefore to be the primary subsets in a three-way classification arranged in any way we please in relation to the Venn diagram. For example, take:



$$x = 2.5.11.17$$
$$y = 3.5.13.17$$
$$z = 7.11.13.17$$

(ii) $\tilde{S}_n \bumpeq S_N - S_n$,

so that, if $\tilde{S}_n \bumpeq S_{n'}$ then n' is the product of all those factors of N which are not factors of n, i.e., $nn' = N$.

(iii)

$$j(x, y) = 2.3.11.13$$
$$j[j(x, y), z] = 2.3.7.17$$
$$j(x, z) = 2.5.7.13$$
$$j[j(x, z), y] = 2.7.3.17.$$

(iv) $\varnothing$

$$S_x \cap S_y \bumpeq S_{5.17}$$
$$S_x \cap \tilde{S}_y \bumpeq S_{2.11}$$
$$\tilde{S}_x \cap S_y \bumpeq S_{3.13}$$

$$\begin{aligned} \tilde{S}_x \cap \tilde{S}_y &\bumpeq S_{1\cdot 7} \\ S_x &\bumpeq S_{2\cdot 5\cdot 11\cdot 17} \\ S_y &\bumpeq S_{3\cdot 5\cdot 13\cdot 17} \\ S_x + S_y &\bumpeq S_{2\cdot 3\cdot 11\cdot 13}\,. \end{aligned}$$

The remaining eight are the complements of these.

In this way an identifying number may be assigned to any subset of a set, namely, the product of a set of primes, the set itself being assigned some (suitably large) square-free number. The relations of any two subsets are then completely determined by the factors of their identifying numbers.

Chapter 6

Exercise 1. The 16 sequences for four lists are:

0 0 0 0	0 0 1 0	0 0 0 1	0 0 1 1
1 0 0 0	1 0 1 0	1 0 0 1	1 0 1 1*
0 1 0 0	0 1 1 0	0 1 0 1	0 1 1 1*
1 1 0 0	1 1 1 0*	1 1 0 1*	1 1 1 1

We wish to select 12 of these sequences in such a way that there are only five 1's in each of the four positions, and can achieve this result by deleting four of the sequences with at least three 1's in each. Let us remove then the four sequences marked * and assign the remaining sequences to the months in order:

Jan.	0 0 0 0	May	0 0 1 0	Sep.	1 0 0 1
Feb.	1 0 0 0	June	1 0 1 0	Oct.	0 1 0 1
Mar.	0 1 0 0	July	0 1 1 0	Nov.	0 0 1 1
Apr.	1 1 0 0	Aug.	0 0 0 1	Dec.	1 1 1 1

The four lists are:

Feb.	Mar.	May	Aug.
Apr.	Apr.	June	Sep.
June	July	July	Oct.
Sep.	Oct.	Nov.	Nov.
Dec.	Dec.	Dec.	Dec.

Exercise 2. (i) For 26 letters we shall require five lists, since $2^4 < 26 < 2^5$; among the 32 characteristic sequences there are five which contain four 1's and one which contains five 1's. If we remove these six we have left the 26 sequences required. In each position there will be sixteen 0's and ten 1's, so that the letter can be identified from five lists each of ten letters. If we assign the sequences to the letters in order, we obtain:

A	0	0	0	0	0	K	0	1	0	1	0	U	1	0	1	0	1
B	1	0	0	0	0	L	1	1	0	1	0	V	0	1	1	0	1
C	0	1	0	0	0	M	0	0	1	1	0	W	0	0	0	1	1
D	1	1	0	0	0	N	1	0	1	1	0	X	1	0	0	1	1
E	0	0	1	0	0	O	0	1	1	1	0	Y	0	1	0	1	1
F	1	0	1	0	0	P	0	0	0	0	1	Z	0	0	1	1	1
G	0	1	1	0	0	Q	1	0	0	0	1						
H	1	1	1	0	0	R	0	1	0	0	1						
I	0	0	0	1	0	S	1	1	0	0	1						
J	1	0	0	1	0	T	0	0	1	0	1						

The lists are:

B	C	E	I	P
D	D	F	J	Q
E	G	G	K	R
H	H	H	L	S
J	K	M	M	T
L	L	N	N	U
M	O	O	O	V
Q	R	T	W	W
S	S	U	X	X
U	V	V	Y	Y
X	Y	Z	Z	Z

(ii) For 52 cards we shall require six lists, and 52 out of the possible 64 characteristic sequences. If the lists are to be made as short as possible, we have to remove

one of the sets of twelve sequences containing the greatest number of 1's, namely (1, 1, 1, 1, 1, 1),

the six sequences containing five 1's, and

five of the fifteen sequences each containing four 1's.

In this way we remove altogether $6+6\times5+5\times4 = 56$ 1's. The total number of 1's in all 64 sequences is 6×32, so that after removing these sequences, we have left altogether 136 1's, and consequently shall finish with four lists of 23 cards each and two lists of 22 cards each, or some more unequal distribution. If we require all lists to be the same length, we remove from the 64 sequences

the six sequences each containing five 1's, and
a set of six of the sequences each containing four 1's and such that there are four 1's in each position, as, e.g.,

$$\begin{array}{cccccc}
1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 .
\end{array}$$

We shall then obtain six lists each of 23 cards.

Exercise 4.

$$(\mathrm{P}_1 \cap \mathrm{P}_2) \cup (\mathrm{P}_3 \cap \mathrm{P}_4) \cup (\mathrm{P}_5 \cap \mathrm{P}_6).$$

$\mathrm{P}_1 \bumpeq \{[n_1] : n_1 = 1+2y+4z+8u+16v+32w\}$

$\mathrm{P}_2 \bumpeq \{[n_2] : n_2 = x+2+4z+8u+16v+32w\}$

so that $\mathrm{P}_1 \cap \mathrm{P}_2 \bumpeq \{[n_{12}] : n_{12} = 3+4z+8u+16v+32w\}$

similarly $\mathrm{P}_3 \cap \mathrm{P}_4 \bumpeq \{[n_{34}] : n_{34} = x+2y+12+16v+32w\}$

and $\quad \mathrm{P}_5 \cap \mathrm{P}_6 \bumpeq \{[n_{56}] : n_{56} = x+2y+4z+8u+48\}$,

i.e., $\quad n_{12} = 3+4r,\ r = 0, \ldots, 15$

$n_{34} = 12+s'+16s,\ s = 0, 1, 2, 3,\ s' = 0, 1, 2, 3$

$n_{56} = 48+t,\ t = 0, \ldots, 15;$

leaving out the elements that are repeated, we may write

$$(\mathrm{P}_1 \cap \mathrm{P}_2) \cup (\mathrm{P}_3 \cap \mathrm{P}_4) \cup (\mathrm{P}_5 \cap \mathrm{P}_6)$$

$$\bumpeq \{[3+4r], [12+s'+16s], [48+t];\ r = 0, 1, 2, 4, 5, 6, 8, 9, 10,\ s' = 0, 1, 2, 3, \quad s = 0, 1, 2, \quad t = 0, \ldots, 15\}.$$

Exercise 5. To express 234, 178 in the binary scale, we divide each repeatedly by 2, and use the successive remainders, thus:

$$\begin{array}{rc@{\qquad\qquad}rc}
234 & & 178 & \\
117 & 0 & 89 & 0 \\
58 & 1 & 44 & 1 \\
29 & 0 & 22 & 1 \\
14 & 1 & 11 & 0 \\
7 & 0 & 5 & 1 \\
3 & 1 & 2 & 1 \\
1 & 1 & 1 & 0 \\
0 & 1 & 0 & 1
\end{array}$$

The subsets with index numbers 234, 178 therefore correspond to the sequences (0, 1, 0, 1, 0, 1, 1, 1)
and (0, 1, 1, 0, 1, 1, 0, 1)
that is, to the unions of the primary subsets
{[1], [3], [5], [6], [7]}
and {[1], [2], [4], [5], [7]}.

Their intersection is therefore $\{ [1], [5], [7] \} \bumpeq \mathrm{A} \cap (\mathrm{B}\, \sigma\, \mathrm{C})$, with index number 162.

Exercise 6. Let the characteristic sequence of one of the primary subsets, say $[n_i]$, contained in Q under the $r-1$ classifications be $(u_1, u_2, \ldots, u_{r-1})$, so that

$$n_i = u_1+2u_2+\ldots+2^{r-2}u_{r-1}.$$

When the new classification giving subsets R and $\tilde{\mathrm{R}}$ is introduced, all the primary subsets constituting R and $\tilde{\mathrm{R}}$ have 1 and 0 respectively as the r-th elements in their characteristic sequences. Since the components $u_1, \ldots, u_{r-1}$ of n_i are determined by the relation of the primary subset $[n_i]$ concerned to the first $r-1$ classifications, they are not affected by the new classification, but the new classification adjoins an r-th component to the characteristic sequences.

Thus

$$[n_i] \cap \mathrm{R} \bumpeq \{[n_i']: n_i' = u_1+2u_2+\ldots+2^{r-2}u_{r-1}+2^{r-1}.1 = n_i+2^{r-1}\},$$

and

$$[n_i] \cap \tilde{\mathrm{R}} \bumpeq \{[n_i'']: n_i'' = u_1+2u_2+\ldots+2^{r-2}u_{r-1}+2^{r-1}.0 = n_i\}.$$

Exercise 7. In Exercise 6 take Q to be the set

$$\mathrm{Q} \bumpeq \mathrm{A}_1+\mathrm{A}_2+\ldots+\mathrm{A}_{r-1}$$

determined by $r-1$ classifications and assume that

$$\mathrm{Q} \bumpeq \{[n]: n = u_1+2u_2+\ldots+2^{r-2}u_{r-1} \text{ and } u_1+u_2+\ldots+u_{r-1} \text{ is odd}\}.$$

Then

$$\tilde{\mathrm{Q}} \bumpeq \{[m]: m = v_1+2v_2+\ldots+2^{r-2}v_{r-1} \text{ and } v_1+v_2+\ldots+v_{r-1} \text{ is even}\}.$$

Now add a new classification giving subsets A_r, $\tilde{\mathrm{A}}_r$. Then

$$\mathrm{A}_1+\mathrm{A}_2+\ldots+\mathrm{A}_{r-1}+\mathrm{A}_r \bumpeq \mathrm{Q}+\mathrm{A}_r \bumpeq (\mathrm{Q} \cap \tilde{\mathrm{A}}_r) \cup (\tilde{\mathrm{Q}} \cap \mathrm{A}_r).$$

The primary subset $[n]$ of Q in the $r-1$ classifications, by Exercise 6, gives the primary subset $[n]$ in $\mathrm{Q} \cap \tilde{\mathrm{A}}_r$ in the r classifications.

The primary subset $[m]$ in $\tilde{\mathrm{Q}}$ under the $r-1$ classifications gives the primary subset $[m+2^r]$ in $\tilde{\mathrm{Q}} \cap \mathrm{A}_r$ under the r classifications.

Thus

$$
\begin{aligned}
\mathrm{Q}+\mathrm{A}_r \bumpeq \{[n], [m+2^r]\colon n &= u_1+2u_2+\ldots+2^{r-2}u_{r-1}+2^{r-1}.0,\\
&\quad u_1+u_2+\ldots+u_{r-1}+0 \text{ is odd},\\
m &= v_1+2v_2+\ldots+2^{r-2}v_{r-1}+2^{r-1}.1,\\
&\quad \text{and } v_1+v_2+\ldots+v_{r-1}+1 \text{ is odd}\}.
\end{aligned}
$$

Since the sets of numbers $\{n\}$ and $\{m\}$ between them contain $2^{r-2}+2^{r-2} = 2^{r-1}$ members, all different, they correspond to the whole set of 2^{r-1} characteristic sequences under r classifications the sum of whose components is odd.

Thus, if under $r-1$ classifications

$$
\begin{aligned}
\mathrm{A}_1+\mathrm{A}_2+\ldots+\mathrm{A}_{r-1} \bumpeq \{[n]\colon n &= u_1+2u_2+\ldots+2^{r-2}u_{r-1}\\
&\quad \text{and } u_1+u_2+\ldots+u_{r-1} \text{ is odd}\},
\end{aligned}
$$

then under r classifications

$$
\begin{aligned}
\mathrm{A}_1+\mathrm{A}_2+\ldots+\mathrm{A}_r \bumpeq \{[n']\colon n' &= u_1'+2u_2'+\ldots+2^{r-1}u_r'\\
&\quad \text{and } u_1'+u_2'+\ldots+u_r' \text{ is odd}\}.
\end{aligned}
$$

But for two classifications

$$\mathrm{A}_1+\mathrm{A}_2 \bumpeq \{[1], [2]\},$$

i.e., the components of the characteristic sequences are (1, 0) and (0, 1), and the assumption is valid. The theorem therefore follows by induction.

Exercise 8. Suppose for any index i

$$
\begin{aligned}
u_i = 0, v_i = 0\colon &\text{ then } \mathrm{F} \not\supset [i], \mathrm{G} \not\supset [i], \mathrm{F}-\mathrm{G} \not\supset [i], \mathrm{G}-\mathrm{F} \not\supset [i],\\
&\quad \mathrm{F}+\mathrm{G} \not\supset [i]\\
u_i = 1, v_i = 0\colon &\text{ then } \mathrm{F} \supset [i], \mathrm{G} \not\supset [i], \mathrm{F}-\mathrm{G} \supset [i], \mathrm{G}-\mathrm{F} \not\supset [i],\\
&\quad \mathrm{F}+\mathrm{G} \supset [i]\\
u_i = 1, v_i = 1\colon &\text{ then } \mathrm{F} \supset [i], \mathrm{G} \supset [i], \mathrm{F}-\mathrm{G} \not\supset [i], \mathrm{G}-\mathrm{F} \not\supset [i],\\
&\quad \mathrm{F}+\mathrm{G} \not\supset [i].
\end{aligned}
$$

Thus if $u_i+v_i = 1$, $\mathrm{F}+\mathrm{G} \supset [i]$

$u_i+v_i = 0$ or 2, $\mathrm{F}+\mathrm{G} \not\supset [i]$,

so that if the sums u_i+v_i are reduced modulo 2 the characteristic sequence of $\mathrm{F}+\mathrm{G}$ is $(\ldots, u_i+v_i, \ldots)$.

This proof applies to a dissection by r subsets independently of r.

Chapter 7

Exercise 1.

Characteristic function of $(A \cup B) \cap (C \cup D)$: $(1+\bar{x}\bar{y})(1+\bar{z}\bar{t})$

Characteristic function of $(A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D)$:

$$
\begin{aligned}
&\equiv 1+(1+xz)(1+xt)(1+yz)(1+yt)\\
&\equiv 1+[1+x(z+t+zt)]\,[1+y(z+t+zt)]\\
&\equiv 1+[1+x+x\bar{z}\bar{t}]\,[1+y+y\bar{z}\bar{t}]\\
&\equiv 1+(\bar{x}+x\bar{z}\bar{t})(\bar{y}+y\bar{z}\bar{t})\\
&\equiv 1+\bar{x}\bar{y}+(x\bar{y}+\bar{x}y+xy)\bar{z}\bar{t}\\
&\equiv 1+\bar{x}\bar{y}+(1+\bar{x}\bar{y})\bar{z}\bar{t}.
\end{aligned}
$$

Exercise 5.

$$
\begin{aligned}
m(x, y) &\equiv c(\bar{x}) \,.\, c(\bar{y})\\
&\equiv n(\bar{x}, \bar{y})\\
&\equiv n[n(x, x), n(y, y)].\\
d(x, y) &\equiv n[n(x, x), y].
\end{aligned}
$$

Exercise 6.

$f(x, y) = 1$	F
x	A
$1+x$	$\tilde{A}$
y	B
$1+y$	$\tilde{B}$
$x+y$	$A+B$
$1+x+y$	$\widetilde{A+B} \bumpeq (A \cap B) \cup (\tilde{A} \cap \tilde{B})$
xy	$A \cap B$
$1+xy$	$\widetilde{A \cap B} \bumpeq \tilde{A} \cup \tilde{B}$
$x+xy$	$A \cap \tilde{B} \bumpeq A-B$
$1+x+xy$	$\widetilde{A \cap \tilde{B}} \bumpeq \tilde{A} \cup B \bumpeq A\,\sigma\,B$
$y+xy$	$B-A$
$1+y+xy$	$B\,\sigma\,A$
$x+y+xy$	$A \cup B$
$1+x+y+xy$	$\tilde{A} \cap \tilde{B} \bumpeq A \downarrow B$

Exercise 7.

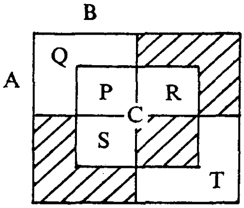
$f(x, y) = 0$	$F \bumpeq \varnothing$	
x	$A \bumpeq \varnothing$	$\tilde{A} \bumpeq U$
$1+x$	$\tilde{A} \bumpeq \varnothing$	$A \bumpeq U$
y	$B \bumpeq \varnothing$	$\tilde{B} \bumpeq U$

$1+y$	$\tilde{B} \bumpeq \varnothing$	$B \bumpeq U$
$x+y$	$A+B \bumpeq \varnothing$	$A \bumpeq B$
$1+x+y$	$\widetilde{A+B} \bumpeq \varnothing$	$A \bumpeq \tilde{B}$
xy	$A \cap B \bumpeq \varnothing$	$A \subseteq \tilde{B}, B \subseteq \tilde{A}$
$1+xy$	$\widetilde{A \cap B} \bumpeq \varnothing$	$A \bumpeq B \bumpeq U$
$x+xy$	$A \cap \tilde{B} \bumpeq \varnothing$	$A \subseteq B$
$1+x+xy$	$\tilde{A} \cup B \bumpeq \varnothing$	$\tilde{A} \bumpeq B \bumpeq U$
$y+xy$	$\tilde{A} \cap B \bumpeq \varnothing$	$B \subseteq A$
$1+y+xy$	$A \cup \tilde{B} \bumpeq \varnothing$	$A \bumpeq \tilde{B} \bumpeq U$
$x+y+xy$	$A \cup B \bumpeq \varnothing$	$\tilde{A} \bumpeq \tilde{B} \bumpeq U$
$1+x+y+xy$	$A \downarrow B \bumpeq \varnothing$	$\tilde{A} \subseteq B, \tilde{B} \subseteq A.$

Exercise 8.

(i) $x+y+z+xyz = 1$ only for (1, 0, 0), (0, 1, 0), (0, 0, 1).

(ii)



Exercise 9.

(ii) $$d(x, y) = \begin{cases} 1 \text{ when } x = 1, y = 0 \\ 0 \text{ otherwise,} \end{cases}$$

so that $d(x, \bar{y}) \equiv m(x, y)$,

i.e., $d(x, y) \equiv m(x, \bar{y}) \equiv x - xy.$

$s(x, y)$

Since $A \,\sigma\, B \bumpeq \widetilde{A-B}$

$$s(x, y) \equiv 1 - d(x, y) \equiv 1 - x + xy.$$

$$n(x, y) = \begin{cases} 1 \text{ when } x = 0, y = 0 \\ 0 \text{ otherwise,} \end{cases}$$

so that $$n(x, y) \equiv m(\bar{x}, \bar{y}) \equiv (1-x)(1-y).$$

(iii) The functions will occur in pairs, in one of which $a = 0$, and the other $a = 1$, according as the value of the function for $(0, 0)$ is 0 or 1. If $dxy+bx+cy = 0$ or 1 then $1-(dxy+bx+cy) = 1$ or 0. We may construct all the functions by first tabulating the functions for which $a = 0$, namely:

$$
\begin{array}{llr}
 & dxy+bx+cy = 0 \text{ or } 1 & \\
(x, y) = & (1, 0) \quad \text{gives} & b = 0 \text{ or } 1 \\
 & (0, 1) & c = 0 \text{ or } 1 \\
 & (1, 1) & b+c+d = 0 \text{ or } 1.
\end{array}
$$

Thus the four possible pairs of entries are:

$b = 0$	$c = 0$	$d = 0$ or 1
0	1	0 or -1
1	0	0 or -1
1	1	-1 or -2,

and the four sets of four functions are:

$(b,c) = (0, 0)$:	0	xy	1	$1-xy$
$(0, 1)$:	y	$y-xy$	$1-y$	$1-y+xy$
$(1, 0)$:	x	$x-xy$	$1-x$	$1-x+xy$
$(1, 1)$:	$x+y-xy$	$x+y-2xy$	$1-x-y+xy$	$1-x-y+2xy$.

We may group these as follows:

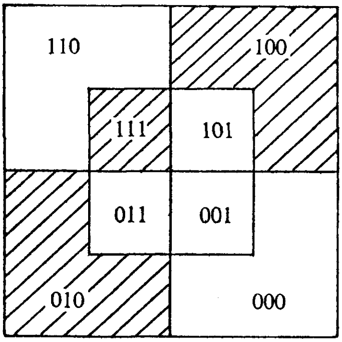
Ø	0
primary subsets	
$\mathrm{A} \cap \mathrm{B}$	xy
$\mathrm{A}-\mathrm{B}$	$x-xy$
$\mathrm{B}-\mathrm{A}$	$y-xy$
$\tilde{\mathrm{A}} \cap \tilde{\mathrm{B}}$	$1-x-y+xy$
union of two primary subsets	
A	x
$\tilde{\mathrm{A}}$	$1-x$
B	y
$\tilde{\mathrm{B}}$	$1-y$
$\mathrm{A}+\mathrm{B}\ (\bumpeq \tilde{\mathrm{A}}+\tilde{\mathrm{B}})$	$x+y-2xy \equiv \bar{x}+\bar{y}-2\bar{x}\bar{y}$
$\tilde{\mathrm{A}}+\mathrm{B}\ (\bumpeq \mathrm{A}+\tilde{\mathrm{B}})$	$1-x-y+2xy \equiv \bar{x}\bar{y}+xy$

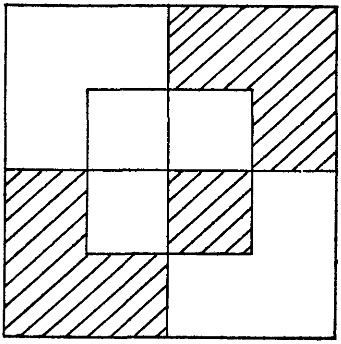
union of three primary subsets

$A \cup B$	$x+y-xy$
$A \, \sigma \, B$	$1-x+xy$
$B \, \sigma \, A$	$1-y+xy$
$\tilde{A} \cup \tilde{B}$	$1-xy$
U	$1.$

(iv) Two such functions are:

$3xyz-2z(x+y)-2xy+x+y$. (8(i)) $x+y+z-2(xy+xz+yz)+3xyz$
represented on the Venn diagram by:





Another is given in Exercise (vi)

(vi)

$$j(x, y) \equiv \begin{cases} 1 \text{ when } (x, y) = (0, 1), (1, 0) \\ 0 \text{ when } (x, y) = (1, 1), (0, 0). \end{cases}$$

Suppose $j(x, y) \equiv axy+bx+cy+d.$

Then

$$\begin{array}{llll} (x, y) = (0, 0); & j(x, y) = 0, & \text{giving} & d = 0 \\ (1, 0) & 1 & & b = 1 \\ (0, 1) & 1 & & c = 1 \\ (1, 1) & 0 & & a = -2, \end{array}$$

so that $j(x, y) \equiv x+y-2xy.$

Given that $j(x, y, z) \equiv j[j(x, y), z]$ etc.,

to prove that $j(x_1, x_2, \ldots, x_r) = \Sigma_1^{(r)}-2\Sigma_2^{(r)}+4\Sigma_3^{(r)}- \ldots$

$$+(-2)^{s-1}\Sigma_s^{(r)}+ \ldots +(-2)^{r-1}x_1x_2 \ldots x_r$$

where $\Sigma_s^{(r)}$ is the sum of the $\binom{r}{s}$ (i.e., ${}^rC_s$) products s at a time of the r variables $x_1, \ldots, x_r$.

Write $\mathrm{J}_s \equiv j(x_1, \ldots, x_s)$, then

$$\begin{aligned}\mathrm{J}_r &\equiv j(\mathrm{J}_{r-1}, x_r) = \mathrm{J}_{r-1} + x_r - 2x_r\mathrm{J}_{r-1} \\ &\equiv \Sigma_1^{(r-1)} - 2\Sigma_2^{(r-1)} + \ldots + (-2)^{(s-1)}\Sigma_s^{(r-1)} + \ldots \\ &\qquad + x_r - 2x_r\Sigma_1^{(r-1)} + \ldots + (-2)^{(s-1)}x_r\Sigma_{s-1}^{(r-1)} + \ldots .\end{aligned}$$

But $(-2)^{(s-1)}\Sigma_s^{(r-1)} + (-2)^{(s-1)}x_r\Sigma_{s-1}^{(r-1)} \equiv (-2)^{(s-1)}\Sigma_s^{(r)}$,

since the first term on the left-hand side contains all the products s at a time that do not include x_r and the second term includes all that do.

Exercise 10. (i) Suppose we have proved the theorem for functions of $r-1$ variables. Any function of r variables can be expressed as

$$h(x_1, \ldots, x_r) \equiv f(x_1, \ldots, x_{r-1}) + x_r\, g(x_1, \ldots, x_{r-1}).$$

Take $x_r = 0$, then if h vanishes for all sequences $(x_1, \ldots, x_{r-1})$ so does f, and it follows that all coefficients in f are zero. Next take $x_r = 1$ and it follows similarly that all coefficients in g are zero. Thus all coefficients in h are zero.

The induction can be founded on

$$\alpha + \alpha_1 x_1 :$$

if this function is zero for $x_1 = 0$ and $x_1 = 1$, then $\alpha = 0$ and $\alpha_1 = 0$.

(ii) There are 2^{2^r} possible functions $f(x_1, \ldots, x_r)$ and 2^{2^r} possible subsets F. Thus either there is one function corresponding to every subset, or some subsets have two functions, and some subsets have none.

Suppose then one subset has two characteristic functions $f(x_1, \ldots, x_r)$ and $g(x_1, \ldots, x_r)$. Then $f-g$ is zero for all sets of values $\{x_1, \ldots, x_r\}$, and therefore has all zero coefficients. That is f and g are the same. Thus every function is the characteristic function of one and only one subset.

(iii) Every subset can be generated from $\mathrm{A}_1, \ldots, \mathrm{A}_r$ by the operations of complementation, intersection, and union, and therefore also by repetitions of the operation represented by $\tilde{\mathrm{A}}_i \cap \tilde{\mathrm{A}}_j$. Thus, from (ii), all functions $f(x_1, \ldots, x_r)$ which have range $\{0, 1\}$ when the variables have domain $\{0, 1\}$ can be generated in the way described.

[*Note*: Using the results of the Appendix (§7.9) we may make theorem (ii) more precise. The matrix equation $\mathbf{w} = \mathbf{Ma}$ establishes a one-to-one correspondence between the set of 2^{2^r} subsets and the set of 2^{2^r} characteristic functions.]

Exercise 11.

$2345 = 1+2+0+0+2^4+2^5+0+0+2^8+0+0+2^{11}+0+0+0+0$, so that the characteristic function is

$$\bar{x}\bar{y}\bar{z}\bar{w}+x\bar{y}\bar{z}\bar{w}+\bar{x}\bar{y}z\bar{w}+x\bar{y}z\bar{w}+\bar{x}\bar{y}\bar{z}w+xy\bar{z}w$$
$$= 1-y-xw-zw+2xyw+xzw+yzw-2xyzw.$$

Check by proving that the values of the function for

$(x, y, z, w) = (0, 0, 0, 0), (1, 0, 0, 0), \ldots, (1, 1, 1, 1)$ are respectively

1 1 0 0 1 1 0 0 1 0 0 1 0 0 0 0

Chapter 8

Exercise 1.

	B	
A	l/N	m/N
	n/N	k/N

$$\mathrm{X} = (l+m)/\mathrm{N}, \quad \mathrm{Y} = (l+n)/\mathrm{N},$$
$$m(\mathrm{X}, \mathrm{Y}) = l/\mathrm{N}, \quad u(\mathrm{X}, \mathrm{Y}) = (l+m+n)/\mathrm{N}$$
$$\mathrm{P}(\mathrm{A}-\mathrm{B}) = m/\mathrm{N} = \mathrm{X}-m(\mathrm{X}, \mathrm{Y})$$
$$\mathrm{P}(\mathrm{A}+\mathrm{B}) = (m+n)/\mathrm{N} = u(\mathrm{X}, \mathrm{Y})-m(\mathrm{X}, \mathrm{Y}).$$

Exercise 2. Subset with index number 234 is

$$\{[1], [3], [5], [6], [7]\} \bumpeq \mathrm{A} \cup (\tilde{\mathrm{A}} \cap \mathrm{B} \cap \mathrm{C}),$$

so that probability is $p_1+p_{23}-p_{231}$.
In the special case probability is $\frac{13}{24}+\frac{1}{6}-\frac{1}{12} = \frac{5}{8}$.
The set is 'all girls together with the right-handed boys wearing spectacles'.

Exercise 3.

$$p_1 = \tfrac{2}{5}, p_2 = \tfrac{2}{7}, p_3 = \tfrac{1}{6}$$

$p_{ij} = p_i p_j$ and $p_{ijk} = p_i p_j p_k$ because events are independent,

so that $\alpha_0 + \Sigma\alpha_i p_i + \Sigma\alpha_{ij} p_{ij} + \alpha_{123} p_{123}$

$$\equiv \alpha_0 + \Sigma\alpha_i p_i + \Sigma\alpha_{ij} p_i p_j + \alpha_{123} p_1 p_2 p_3$$
$$\equiv f(p_1, p_2, p_3).$$

For the set with index number 234

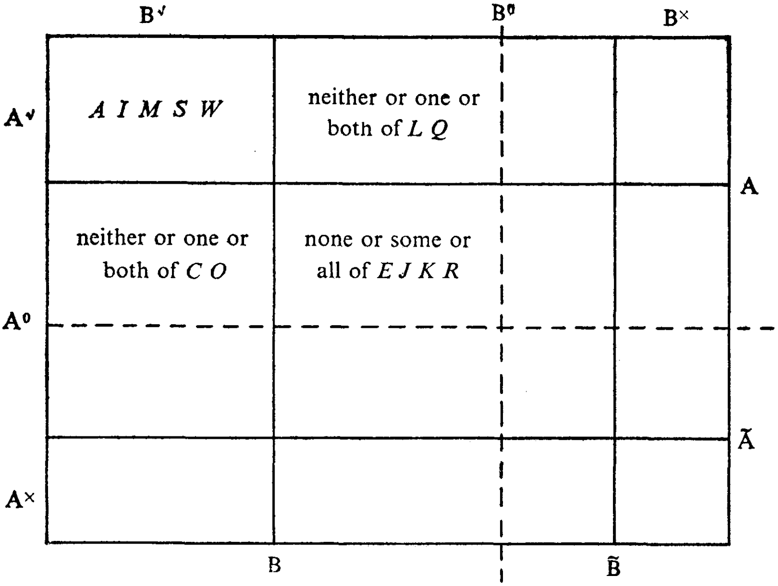
$$f(x, y, z) \equiv x + yz - xyz$$

so that probability $= \frac{2}{5} + \frac{1}{21} - \frac{2}{105} = \frac{45}{105} = \frac{3}{7}$.

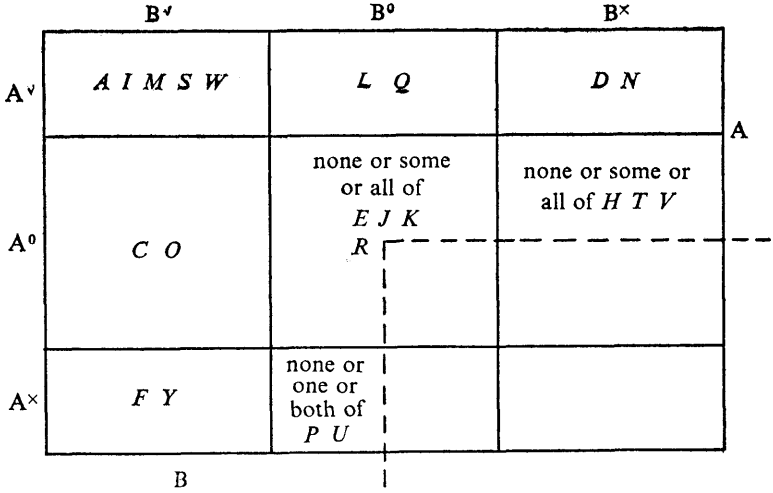
Exercise 4.

The characteristic function is $f(x, y) \equiv \xi_2^T \mathbf{a} \equiv \xi_2^T\, \mathbf{M}_2^{-1}\mathbf{w}$. For the probability, 1, x, y, xy are respectively replaced by 1, p_1, p_2, p_{12}, so that the probability is $[1, p_1, p_2, p_{12}]\, \mathbf{M}_2^{-1}\mathbf{w}$.

Exercise 5. (i) $\mathrm{A}^{\surd} \cap \mathrm{B}^{\surd} \bumpeq (\mathrm{A} \cap \mathrm{B})^{\surd}$


B√
B⁰
B×
A√
A I M S W
neither or one or both of *L Q*
A
neither or one or both of *C O*
none or some or all of *E J K R*
A⁰
Ã
A×
B
B̃

$$\mathrm{A}^{\surd} \cap \mathrm{B}^{\surd} \bumpeq \{A, I, M, S, W\}$$
$$\bumpeq (\mathrm{A} \cap \mathrm{B})^{\surd}.$$



	$B^{\surd}$	B^{0}	$B^{\times}$
$A^{\surd}$	*A I M S W*	*L Q*	*D N*
A^{0}	*C O*	none or some or all of *E J K R*	none or some or all of *H T V*
$A^{\times}$	*F Y*	none or one or both of *P U*	

$A^{\surd} \cup B^{\surd} \bumpeq \{A, I, M, S, W, C, O, F, Y, L, Q, D, N\} \bumpeq (A \cup B)^{\surd}$.

Exercise 9.

$$B^{\surd} \cap A^{*} : \tfrac{1}{2}[(y-y^2)+(-x^2-x^2)+(-x^2y+x^2y^2)] \equiv \tfrac{1}{2}(1-x^2)(y-y^2)-x^2.$$

$\tfrac{1}{2}(1-x^2)(y-y^2) = 0$ when $y = x, 1-x^2, -x, -x^2$ or $1-y^2$ so that $A^{*} \cap (A^{\surd}, A^{0}, A^{\times}, A^{*}, B^{0}) \bumpeq A^{*}$.

Exercise 10.

$A^{0} \cap (A^{\surd}, A^{\times})$:

$$\tfrac{1}{2}[(1-x^2)-(1-x^2)+(\pm x-x^2)\pm x(1-x^2)+x^2(1-x^2)] \equiv \tfrac{1}{2}(\pm x-x^2).$$

Exercise 13.

(i) $(A\,\sigma\,B)^{\surd} \bumpeq (\tilde{A} \cup B)^{\surd} \bumpeq A^{\times} \cup B^{\surd} : -\mu(x, -y)$

$(B\,\sigma\,A)^{\surd} : \quad -\mu(-x, y)$

$(A \cap B)^{\times} \bumpeq A^{\times} \cup B^{\times} : \quad -\mu(x, y)$

(ii) $(A+B)^{\surd} \bumpeq (A \cap \tilde{B})^{\surd} \cup (\tilde{A} \cap B)^{\surd} \bumpeq (A^{\surd} \cap B^{\times}) \cup (A^{\times} \cap B^{\surd})$

$(A+B)^{\times} \bumpeq (A \cap \tilde{B})^{\times} \cap (\tilde{A} \cap B)^{\times} \bumpeq (A^{\times} \cup B^{\surd}) \cap (A^{\surd} \cup B^{\times})$

$x \backslash y$	1	0	-1
1	-1	0	1
0	0	0	0
-1	1	0	-1

Substitution in the general symmetric form in two variables gives the required result.

Exercise 14.

$$\tfrac{1}{4}(1+x)(1+y)(1+z)[1+(1-x)(1-y)+(1-x)(1-z)+(1-y)(1-z)]-1$$

$$= \begin{cases} -1 \text{ whenever } x=-1 \text{ or } y=-1 \text{ or } z=-1 \\ 0 \begin{cases} \text{for } x=y=0,\ z=1 \text{ and symmetrically} \\ \text{for } x=0,\ y=z=1 \text{ and symmetrically} \end{cases} \\ 1 \text{ only when } x=y=z=1. \end{cases}$$

$$\begin{aligned} v(x,y,z) &\equiv v[v(x,y),z] \equiv -\mu[+\mu(-x,-y),-z] \\ &\equiv -\mu(-x,-y,-z). \end{aligned}$$

Exercise 15.

$$\begin{aligned} A^{\times} \cap B^{0}: \quad & \tfrac{1}{2}[-x-x^2+(1-y^2)-(1-y^2)^2-x(1-y^2)+x^2(1-y^2)] \\ & \equiv \tfrac{1}{2}[-(x+x^2)+(-x+x^2)(1-y^2)] \\ & \equiv -x-\tfrac{1}{2}(x^2-x)y^2. \\ A^{\surd} \cup B^{0}: \quad & \tfrac{1}{2}[x+x^2+(1-y^2)+(1-y^2)^2-x(1-y^2)-x^2(1-y^2)^2] \\ & \equiv \tfrac{1}{2}[x+x^2+2(1-y^2)-(x+x^2)(1-y^2)] \\ & \equiv 1-y^2+\tfrac{1}{2}y^2(x^2+x). \end{aligned}$$

$A^{\times} \cap B^{0}$

$x \backslash y$	1	0	−1
1	−1	−1	−1
0	0	0	0
−1	0	1	0

$A^{\surd} \cup B^{0}$

$x \backslash y$	1	0	−1
1	1	1	1
0	0	1	0
−1	0	1	0

Exercise 16.

The function is $v[\mu_{\surd 0}(x,y),\ \mu_{\times 0}(x,y),\ \mu_{00}(x,y)]$ and corresponds to $(A^{\surd} \cap B^{0}) \cup (A^{\times} \cap B^{0}) \cup (A^{0} \cap B^{0}) \mathrel{\hat{=}} B^{0}$.

Exercise 17.

$$\begin{aligned} A^{\surd} \cap B^{*}: \ & \tfrac{1}{2}(x-y^2-x^2-y^2-xy^2+x^2y^2) \\ & \equiv -y^2-\tfrac{1}{2}(x^2-x)(1-y^2). \end{aligned}$$

$A^{0} \cap B^{*}$: replace x by $1-x^2$; second term is zero: $-y^2$ so that $A^{0} \cap B^{*} \mathrel{\hat{=}} B^{*}$.

$A^{*} \cap B^{*}$: replace x by $-x^2$: $-x^2-y^2+x^2y^2$.

$$A^{\surd} \cup B^* : \tfrac{1}{2}(x - y^2 + x^2 + y^2 + xy^2 - x^2y^2)$$
$$\equiv \tfrac{1}{2}[(x^2 + x) - (x^2 - x)y^2].$$

$A^0 \cup B^*$: replace x by $1 - x^2$: second term is zero : $1 - x^2$
so that $A^0 \cup B^* \bumpeq A^0$.

$A^* \cup B^*$: replace x by $-x^2$: $-x^2y^2$.

$A^{\surd} \cap B^*$			$A^* \cap B^*$			$A^{\surd} \cup B^*$			$A^* \cup B^*$		
−1	0	−1	−1	−1	−1	1	1	1	−1	0	−1
−1	0	−1	−1	0	−1	0	0	0	0	0	0
−1	−1	−1	−1	−1	−1	−1	0	−1	−1	0	−1

INDEX

Abel, 183
Algebra, 71
Algebra
  binary, 103
  Boolean, 71
  of subsets ('set-algebra'), 71
  statement, 62
  ternary, 147
Algebraic model for Boolean algebra, 120
Algebraic number(s), 181, 184
  of degree n, 184
  set of, 184
Arrangement of the elements of a set, 174
Associative operation, 24
  and use of parentheses, 23-4
Axiom system
  complete, 71
  consistent, 71
  independent, 71
Axiom system for
  an algebraic model for Boolean algebra, 121-2
  binary algebra, 104
  Boolean algebra, 71
  set-algebra when allowing for ignorance, 143-6
  ternary algebra, 148

Basic set, 6
Biconditional statement, 61
Binary algebra, 103
  and set operations, 105
  and set relations, 111
  axioms for, 104
Binary characteristic function(s), 116
  and set operations, 105-6
  corresponding to a dissection by n subsets, 114
  of a subset, 114
Binary notation, 91
  reversed, 91
Binary numbers and characteristic sequences, 96
Binary relation, 67
Boolean Algebra, 71
  algebraic model for, 120
  axioms for, 71
  deduced from ternary algebra, 158
Braces (use as set notation), 6
Brouwer, 191

Cantor, 189
Cardan 182
Cartesian
  co-ordinates, 101
  product set, 102
Characteristic function(s)
  and matrix algebra, 122
  coefficient vector corresponding to, 122
  synthesis and analysis of, 118
Characteristic sequence(s)
  and binary numbers, 96
  of a subset, 97
Characteristic functions, ternary, 148-9
Closed operation, 68
Commutative operation, 20
Complement
  of a subset, 29
  of unions and intersections, 30
Condition(s)
  necessity, 53
  necessary and sufficient, 54
  sufficiency, 52
Conditional statement, 59
Conjunction of two statements, 49
Construction of a mathematical model, 69
Converse of a relation, 55
Counting numbers, 166
  three ways of using, 166
  set N of, 167
Cubic equations and polynomials, 181-2

Decimal representation of real numbers, 168
Demonstrating a proof, 14
Denumerability of
  any non-finite subset of N, 173
  set of algebraic numbers, 184
  set of counting-number pairs, 174
  set of integers, 174

Denumerability of—*continued*
  set of rationals, 175
  set of r-plets of counting numbers, 176
Denumerable set, 174
Descartes, 127, 128
Descriptions and statements, 47
Diagrams
  introduction of, 10-14
  Venn, 14
  use of, 14, 30
Disjunction of two statements, 50
Distributive property of operations, 36
  left, 213
  right, 213
Direct method of proof, 56
Duality principle, 44
  for set algebra, 43
  for Boolean algebra, 72

Element of a set, 6
Empty set, 21
Equivalent statements on a set, 55
  necessary and sufficient conditions and, 55
Euler's constant, 189

Factorisation as a sorting process, 78
Fibonacci numbers, 171
Fictitious subsets, 151-2
Formal solution of algebraic equations
  of degree 2, 3 or 4, 179-83
  of degree $n > 5$, 184
Formulation of a mathematical system, 44
Fundamental theorem of algebra, 183

Geometrical significance of denumerability of Q, 177

H.C.F. and L.C.M., 78-87
H.C.F. (highest common factor), 79
Height of a polynomial, 186
Hermite, 189

Implies, 53
  logician's use of, 58
Inclusion relation for subsets, 8
  as a partial ordering, 73
  interpreted in statement algebra, 51
Independent probabilities, 132
Index number of a subset, 98
Index vector of a subset, 122
Indirect method of proof, 57
Intersection operation on subsets, 19-26

L.C.M. (least common multiple), 82
Labelling by binary numbers, 90
Liouville, 189
Lindemann, 189
Logician's term 'implies', 58

Modified Venn diagram, 142

Necessary and sufficient conditions, 54
Necessity conditions, 53
Negation of a statement, 47
Newton, 127, 128
Non-denumerable sets, 179
Non-finite sets, 163
Notation used to specify a set, 6, 92 (footnote)
Nugatory function $n(x, y)$, 110
Null set, 21

One-to-one correspondence, 164
  as a relation on sets, 165
Operation defined by specifying its properties, 68
Order relation, 73
  partial, 73

Parentheses
  associative operations and, 24, 28
  used to specify order of execution of operations, 23-4, 33, 40
Partial ordering, 73
Permutation of a finite set, 171
  complete, 172
Polynomial
  equations, 181-4
  height of, 186
Prescription of non-finite subsets of a set, 169-72
Primary subset(s) of a set, 41
  characteristic sequence corresponding to, 98
  characteristic function corresponding to, 118
  number of, 41

Probabilities, 131
  characteristic functions and, 136
  independent, 132
Proper subset of a set, 9
Pythagoras' theorem, 18

Quadratic equations and surds, 179
Quartic equations, 182-3

Rational characteristic functions, 116-18
  and matrix algebra, 122
  and probabilities, 138
  synthesis and analysis of, 118
Real numbers, 168
  decimal representation of, 168
Recurrence relation, 171
Reflexive property of a relation, 67
Relation
  binary, 67
  converse of a, 55
Relation
  'belongs to' or 'is an element of', 7
  'may be replaced by', 66
  'is contained in', 8
  'is in one-to-one correspondence with', 165
  'is the same set as', 8
  'is the same statement as', 48
Relative complement of a subset, 38

Set(s), 5
Set-algebra, 71
  definitions and table of results, 44-6
  when allowing for ignorance, 140-6
Set-difference operation, 38
Set notation, 6
Set operations, 19-46
  and binary algebra, 111
  and ternary algebra, 157
  when allowing for ignorance, 140-6
Set relations and binary algebra, 111
  and ternary algebra, 157
  when allowing for ignorance, 145
Sets and binary arithmetic, 88
Sigma operation, 39
Sorting processes, 1-5
Statement(s), 47
Statement(s)
  biconditional, 61
  conditional, 59
  conjunction of, 49
  disjunction of, 50
  negation of a, 47
Subset formation and set operations, 29
Subset of a set, 5
Sufficiency conditions, 53
Symbols
  introduction of, 5
  use of, 17, 34
Symmetric-difference operation, 74
Symmetric property of a relation, 67

Tangible subset, 152
Ternary algebra
  and characteristic functions, 148
  and set operations, 157
  and Boolean algebra, 158
  as a model for set-algebra when allowing for ignorance, 147-57
Transcendental number, 181
Transitivity of a relation, 16

Unary operation, 68
Union operation, 26-9
Universal set, 6

Venn diagrams, 14
  modified, 142

THIS BOOK is designed to have a wide appeal, the authors having assumed in the reader no more than a knowledge of school mathematics. The general approach to the subject is a new one, as are the methods used to tie in the various algebraic models. The book should prove particularly useful to teachers, to students in the senior forms of schools and in the early years of university study, and it should appeal strongly to general readers.

The purpose of the book is to develop in the reader an appreciation of the genesis and evolution of mathematical ideas. By means of illustrations drawn from the small and easily comprehended field of finite set relations, it illustrates the way in which mathematics develops from its origins in the co-ordination of physically observed relations. This development is then traced through the representation of these relations by various mathematical models up to the evolution of branches of pure mathematics which bear little trace of their practical beginnings. The final chapter leads the reader towards the theory of infinite sets.

T. G. ROOM, F.R.S. is Professor of Mathematics (Pure Mathematics) and Dean of the Faculty of Science at the University of Sydney, and J. M. MACK is a Lecturer in Mathematics at the same University.

Australia $3.00 Sterling 24s. net

THE SORTING PROCESS

Room and Mack

SYDNEY